Performance and Security Analysis of Parameter-Obfuscated Analog Circuits

Vaibhav Venugopal Rao, *Student Member, IEEE*, and Ioannis Savidis, *Senior Member, IEEE*

***Abstract*— In this article, key-based obfuscation of the transistor dimensions is proposed to mask the biasing conditions of an analog circuit and, therefore, protect the circuit against intellectual property (IP) piracy. Vector- and mesh-based obfuscations are developed that provide different degrees of circuit security with tradeoffs in design complexity and area. An algorithm for the selection of an obfuscation transistor and a satisfiability modulo theory (SMT)-based algorithm that searches the design space to determine the dimensions of the obfuscation transistors are developed to reduce the computational complexity of designing and implementing the proposed parameter obfuscation techniques. The parameter obfuscation techniques, along with the developed algorithms, are implemented on an active inductor-based second-order bandpass filter (BPF) and an operational amplifier (op-amp). The results from the analysis of the obfuscated BPF and op-amp indicate that the critical circuit performances are properly locked with at least 15% variation from the target circuit parameters when setting incorrect transistor sizes. A simulation-based optimization algorithm is proposed to tune the biasing conditions and transistor body voltages, which mitigates the effects of both the parasitic impedance of the circuit and any variation due to the implementation of the obfuscation circuitry. The proposed simulation-based optimization algorithm determines the biasing conditions and body voltages of the BPF in 500 iterations and the op-amp circuit in 70 iterations, which provides a significant reduction in the design time and the number of circuit recycles. Implementing the parameter obfuscation technique with the proposed algorithms provides an efficient means to secure analog circuits while reducing the design time to implement security features.**

***Index Terms*— Analog obfuscation, analog security, satisfiability (SAT) modulo theory (SMT).**

I. Introduction

THE increasing demands from the automotive industry, applications based on the Internet of Things (IoTs), 5G communication, and, more generally, analog computation have fueled the growth in the use of analog integrated circuits (ICs) [1]–[3]. Due to the growing demand for analog circuits in various product sectors, the market for analog ICs is expected to register a cumulative annual growth rate of 5.5% from 2019 to 2024 [1]. To meet the growing demand and to gain the first-mover advantage in the analog IC market, fabrication and packaging through the use of off-shore facilities are often utilized [4], which has also resulted in an increased security risk to the IC supply chain [5]. The increased vulnerabilities of an analog circuit coupled with the greater complexity in circuit design, increased risk of failure, lack of sophisticated analog EDA tools, and greater rewards when achieving first mover advantage have led to increased attacks. As described in [6], analog circuits are the most forged ICs and account for nearly 25% of all counterfeit semiconductor electronics.

In this article, key-based parameter obfuscation techniques are proposed to protect analog circuits against intellectual property (IP) piracy. In addition, an algorithm for the selection of obfuscation transistors, a satisfiability modulo theory (SMT)-based algorithm to determine the sizes of the obfuscation transistors, and a simulation-based post-obfuscation and post-fabrication tuning optimization algorithm are developed to reduce design complexity and efficiently implement the proposed parameter obfuscation techniques. The primary contributions of this article include

1) A key-based parameter obfuscation technique that masks the biasing conditions and target performance metrics of an analog IC based on applied keys.
2) The development of an algorithm for the selection of obfuscation transistors and an SMT-based algorithm for determining the sizes of obfuscation transistors, where the principle innovations include
   a) an efficient integration of the parameter obfuscation technique during the design phase of an analog circuit to minimize complexity and reduce overall design time, and
   b) a means to auto-determine and size the transistor(s) that effectively mask the performance parameters of the circuit, and
3) The development of a simulation-based optimization technique to mitigate the impact of both the parasitic impedance of the circuit and any process, voltage, and temperature (PVT) variations, including from the implementation of the parameter obfuscation techniques.

The rest of the article is structured as follows. Prior work on the security of analog ICs is discussed in Section II. The assumed threat model for the parameter obfuscation techniques is described in Section III. An overview of the proposed parameter obfuscation techniques is provided in Section IV. The challenges of implementing the parameter obfuscation techniques and the developed solutions to address the chal-

Manuscript received December 21, 2020; revised May 7, 2021 and June 26, 2021; accepted July 26, 2021. Date of publication October 26, 2021; date of current version November 30, 2021. This work was supported in part by Drexel Ventures Innovation Fund and in part by the National Science Foundation under Grant CNS-1751032. *(Corresponding author: Vaibhav Venugopal Rao.)*

The authors are with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA 19104 USA (e-mail: vv85@drexel.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TVLSI.2021.3109062.

Digital Object Identifier 10.1109/TVLSI.2021.3109062

lenges are described in Sections V and VI, respectively. The implementation of the parameter obfuscation techniques and the proposed algorithms on a bandpass filter (BPF) and an operational amplifier (op-amp) is described in Section VII. The execution of the simulation-based optimization algorithm that mitigates the effects of both the parasitic impedance of the circuit and any PVT variations on the circuit, including from the implementation of the obfuscation techniques, is described in Section VIII. The metrics used to compare the performance of the obfuscated circuit and the security provided by the developed parameter obfuscation techniques to methods described in the literature that obfuscate analog circuits are provided in Section IX. A discussion on the effect of parameter obfuscation on design complexity and the occupied circuit area is provided in Section X. Concluding remarks are provided in Section XI.

II. Prior Work

Circuit techniques to protect analog IP from various security threats are still in early development. However, some early research on securing analog mixed-signal and RF circuits has been reported [7]. Split manufacturing is one of the first techniques proposed to prevent the piracy of an analog IC [8]. With split manufacturing, the fabrication of an analog IC is divided between a front-end-of-line (FEOL) process consisting of transistor layers fabricated by an untrusted foundry and a back-end-of-line (BEOL) process consisting of metallization layers fabricated by a trusted foundry. By splitting the manufacturing process, the design details and specifications are not fully disclosed to an untrusted foundry, which requires exploration of a large design space to completely reverse engineer the analog IC. Split manufacturing is effective against reverse engineering from an untrusted foundry only during fabrication and does not prevent IP piracy from an untrusted end user.

A key-based locking mechanism for a sense amplifier circuit is proposed in [9]. A memristor crossbar structure is used to program the voltage divider circuit, where the crossbar is configured properly only when the correct key is applied. The practical application of the technique is limited as memristors are not readily available across fabrication technologies, and the memristor fabrication process is incompatible with the standard CMOS fabrication process.

The use of a fabrication process that includes multi-threshold voltage (V_{TH}) transistor is proposed to protect analog ICs from reverse engineering [10]. A small number of nominal V_{TH} (NVT) transistors are replaced with low V_{TH} (LVT) and/or high V_{TH} (HVT) transistors while maintaining the target performance specifications of the circuit. The primary drawback of implementing multithreshold voltages as a security feature is that the technique is only applicable to large analog circuits as the threshold voltage for smaller circuits with few transistors is relatively easy to determine using a brute-force attack. In addition, the use of scanning electron microscopy (SEM) [11] and passive voltage contrast [12] have been shown to determine the dopant concentration of the silicon, which reveals the threshold voltage of the transistors.

A more general key-based locking mechanism for analog circuits is proposed in [13]–[17], where additional locking circuitry is inserted into the IC. A locked design produces a correct output only on the application of the correct key. In [13] and [14], the sizes of the biasing transistors are obfuscated using a key, and only on the application of the correct key are the correct biasing conditions set that result in proper circuit functionality. In [15], combinational logic locking is applied to the current mirrors of the circuit, where transistors of different sizes are used to mask the current gains. The primary disadvantage of applying combinational locking to the current mirrors is that the technique only masks the biasing currents of an analog circuit. The technique described in [16] and [17] obfuscates the digital blocks of an analog mixed-signal (AMS) IC through the implementation of stripped-functionality logic locking (SFLL). The disadvantage of obfuscating only the digital components of an AMS IC is that the purely analog components are not protected. In addition, the tuning range of the circuit parameters, as described in [16], is limited by the number of passive components in the resistor or capacitor banks. The attacker is able to reduce the search space by analyzing only the passive components and determine the combination of passive components that result in the optimal circuit performance irrespective of the size of the key. To increase the tunable range of each performance parameter, the total aggregate of passive components must be increased, which results in a greater overhead in the area of the circuit as compared to obfuscating active transistors.

III. Threat Model

An untrusted foundry model is assumed, where the foundry has access to the circuit design and possesses the necessary tools and skills to counterfeit and overproduce the IC from the provided GDS-II file [18]. In addition, the circuit is assumed trusted and devoid of any malicious components when in the design phase. An additional threat model considered is an untrusted end user, where the adversary has access to the primary key inputs that, based on a given applied key, alter the response of the circuit. Note that analog circuits are typically a part of a much larger system, which limits the probing of internal node voltages and currents. Therefore, an adversary is assumed unable to determine the internal node voltages and currents of the circuit.

IV. Parameter Obfuscation

Applying the parameter obfuscation technique involves replacing a single (or multiple) transistor(s) in an analog circuit with an array of obfuscation transistors of different sizes that are controlled by a digital key. The strong correlation between the biasing conditions and the performance of an analog circuit is utilized when securing analog components with the parameter obfuscation technique. Based on the applied key sequence, which sets the transistor dimensions, the biasing conditions and performances of the circuit are set, with only the correct key sequence resulting in the target biasing conditions. The technique is applicable to setting the voltage at a node, the current through a node, and/or modifying the gain of the circuit. The parameter obfuscation technique has been implemented with both vector- and mesh-based configurations [14].

A. Vector-Based Parameter Obfuscation

The topology of the vector-based parameter obfuscation technique is shown in Fig. 1. A single transistor is replaced by multiple transistors of the same length but of different widths placed in parallel, with each parallel transistor controlled by

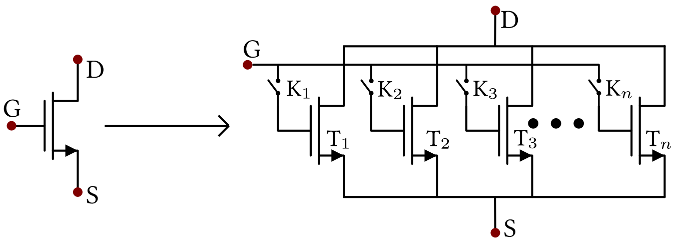


Fig. 1. Schematic of vector-based parameter obfuscation implemented on a single transistor.

an independent key bit. When a digital bit is set to logic high, current flows through the corresponding parallel transistor. The total current through the parallelized transistor depends on the effective total width of the obfuscated transistor set by the applied key, where the total current converging at node S is equal to the sum of the activated transistor paths (the on paths) [13]. Only on the application of the correct n-bit key, are the target transistors turned on, which results in the desired currents and target performance parameters.

The original width that produces the target current is divided into multiple target transistor widths of smaller dimension that when all are properly activated result in the original target current. *Obfuscation transistors* are also added in parallel to mask the target width. The effective current through the vector obfuscated transistor is given by

$$I_{\text{vector}} = \sum_{i=1}^{n} I_i K_i, \tag{1}$$

where I_i is the drain to source current of the ith parallel transistor and $K_i \in \{0, 1\}$ represents a single digital key bit applied to the ith transistor. The effective current I_{vector} is equivalent to the sum of the currents through the active transistor paths when the applied key bits K_i are 1. Under ideal conditions, $K_p = \mu C_{\text{ox}}$ and voltages V_{GS}, V_T, and V_{DS} are equal among all parallel transistors. Therefore, the cumulative effective width over length ratio T_{vector} of the activated transistors for the vector-based obfuscation technique is given by

$$T_{\text{vector}} = \sum_{i=1}^{n} T_i K_i, \tag{2}$$

where $T_i = (W/L)_i$ is the width over length ratio of the ith transistor. As the transistor lengths are kept constant, the $(W/L)_i$ ratio is dependent solely on the transistor width W_i.

B. Mesh-Based Parameter Obfuscation

The implementation of the mesh-based obfuscation technique on a single transistor is shown in Fig. 2. Adding transistors in parallel leads to an increase in the overall transistor width while keeping the length constant, whereas adding transistors in series results in a composite structure that effectively increases the transistor length [14].

For a series-connected composite transistor, the topmost transistor of the stack typically operates in saturation, while the remaining transistors operate in linear mode. The overall effective current through a series-connected transistor of m rows is given by

$$I_{\text{series}} = \frac{1}{2}\left(\frac{1}{\beta_1} + \frac{1}{\beta_2} + \cdots + \frac{1}{\beta_m}\right)^{-1} \cdot (V_{\text{GS}'} - V_T)^2, \tag{3}$$

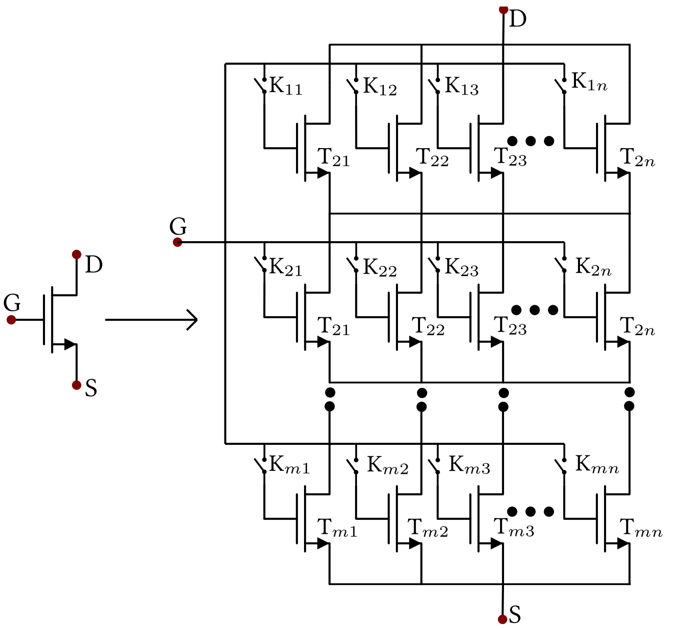


Fig. 2. Schematic of mesh-based parameter obfuscation implemented on a single transistor.

where β is the product of the electron mobility μ, oxide capacitance C_{ox}, and the transistor width over length ratio T. The $V_{\text{GS}'}$ and V_T terms are the gate to source voltage and threshold voltage of the top most transistor, respectively. Based on (3), the effective width over length ratio of the series connected transistor T_{series} is given by

$$\frac{1}{T_{\text{series}}} = \frac{1}{T_1} + \frac{1}{T_2} + \cdots + \frac{1}{T_m}. \tag{4}$$

The primary advantage of using the mesh-based obfuscation technique as compared to vector-based obfuscation is that, in addition to masking the transistor dimensions, the threshold voltage and small-signal parameters of a transistor are also masked. Therefore, an adversary must determine both the biasing conditions and the small-signal parameters to properly set the target transistor dimensions. Similar to the vector-based technique, *obfuscation transistors* are added to mask the *target transistors*, and the activation of each transistor of the mesh is controlled by a single dedicated key bit $K_{ij} \in \{0, 1\}$. Therefore, the effective width over length ratio of the mesh transistor T_{mesh} consisting of m rows and n columns, as shown in Fig. 2, and for an applied key K is given by

$$\frac{1}{T_{\text{mesh}}} = \sum_{i=1}^{m}\left(\frac{1}{\sum_{j=1}^{n} T_{ij} K_{ij}}\right), \tag{5}$$

where for each row $i \in \{1, 2, \ldots, m\}$,

$$\sum_{j=1}^{n} K_{ij} \geq 1. \tag{6}$$

Applying (6) ensures that at least one j^{th} column of n total columns in each row i is activated. Only on the application of the correct key, are the target transistors turned on, which contributes to the desired current and small-signal parameters that set the target performance of the obfuscated transistor. As the voltage at the source of the component transistor(s) nearest to the drain terminal of the composite transistor

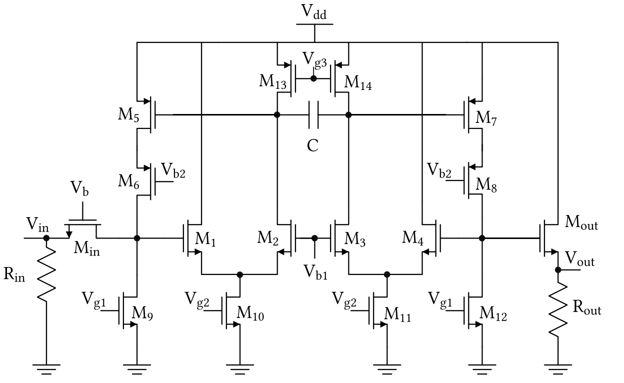


Fig. 3. Circuit schematic of an active inductor-based second-order BPF.

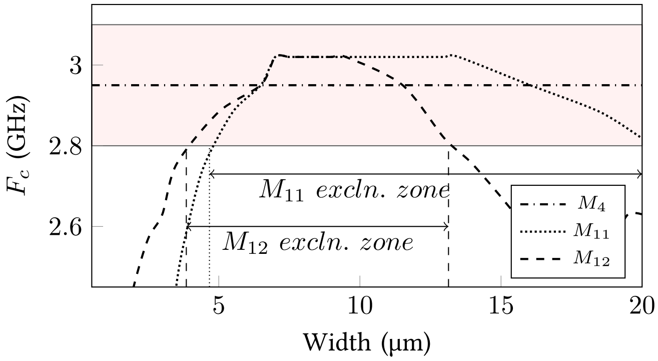


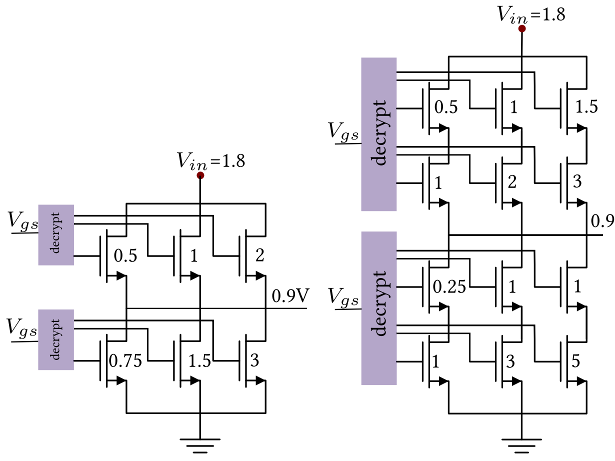
Fig. 4. Characterization of the center frequency of the BPF for widths of 0.5 μm to 20 μm for transistors M_4, M_{11}, and M_{12}.

increases due to the stacking effect, the number of rows in the mesh is limited by $V_{\mathrm{GS}} - m \cdot V_{\mathrm{th}} \geq 0$ for m number of rows.

V. Challenges With Parameter Obfuscation

The implementation of the parameter obfuscation techniques on an analog circuit poses design challenges. One of the primary design challenges is the drift in the performances of the analog circuit due to the parasitic impedances and non-linearities that result from the inclusion of both the *obfuscation* and *target* transistors and the switches implementing the key-bits. Therefore, additional steps are needed to assure that the target performance specifications of the circuit are satisfied while compensating for the added parasitic impedances and non-idealities resulting from the implementation of the obfuscation techniques.

Additional design challenges specific to the implementation of the parameter obfuscation techniques include: 1) the determination of the transistor(s) to obfuscate in the analog circuit, 2) the presence of multiple correct keys, and 3) the possibility of incorrect keys resulting in "good enough" circuit functionality (performance close to the target specifications). The variation in the center frequency F_c of the active inductor-based second-order BPF shown in Fig. 3 for widths of 0.5 μm to 20 μm for transistors M_4, M_{11}, and M_{12} is shown in Fig. 4. The size of transistor M_4 has no effect on the F_c of the BPF, which indicates that M_4 is not an appropriate selection for the implementation of the obfuscation technique. The size of transistors M_{11} and M_{12} produces exclusion zones of 15.33 μm and 9.3 μm, respectively, for ±5% variation in the target F_c. The characterization of F_c indicates that transistor M_{12} produces the smallest exclusion zone and ensures a wider range of *obfuscation transistor* sizes as compared to transistor M_{11} and is, therefore, better suited for obfuscation. The analysis of the results shown in Fig. 4 indicates that proper obfuscation of the transistors of an analog circuit must be completed to effectively mask the target transistor sizes and, therefore, the performance specifications of the circuit.



(a) (b)

Fig. 5. Circuit schematic of implementing (a) vector- and (b) mesh-based obfuscation on a voltage divider circuit that produces a target output voltage of 0.9 V. Transistor width over length (W/L) ratios and applied voltages are provided in the figure.

TABLE I

Characterization of the Output Voltage for Different Key Sequences Applied to the Voltage Divider Circuit Shown in Fig. 5 Obfuscated by the Vector- and Mesh-Based Techniques

Vector Based Obfuscation		
Key 1	Key 2	V_{out}
110	010	0.9
011	001	0.9
010	100	1.01
001	110	0.85

Mesh Based Obfuscation		
Key 1	Key 2	V_{out}
110001	011010	0.9
101010	101001	0.9
010100	111100	1.02
001001	101010	0.85

The implementation of the proposed obfuscation technique on a voltage divider is shown in Fig. 5, with results from the analysis of the voltage at the output node of the divider listed in Table I. The two key sequences listed in rows 1 and 2 of Table I for both the vector- and mesh-based obfuscated voltage divider circuit produce the desired output voltage of 0.9 V. In addition, the keys listed in rows 3 and 4 produce voltages that are close to the desired output voltage of 0.9 V. The results listed in Table I highlight the challenge of producing a unique key when obfuscating analog parameters.

Three design criteria are proposed to address the challenges of implementing the obfuscation techniques: (1) determine the proper transistor(s) in the circuit to obfuscate, (2) ensure the proper subdivision of the width and length of the *target transistors*, and (3) determine the proper size of the *obfuscation transistors*. The primary constraints of criteria (2) and (3) include: 1) the generation of a single correct key and 2) the circuit performances that are set by applying the closest incorrect key must result in at least a target percentage difference from the specified circuit performances produced by the correct key.

Algorithm 1 Selection of the Transistor(s) to Obfuscate by Sorting the Obfuscation Range of the Transistors in Decreasing Order

```
Input: $T_{array}$, $P_T$, $var$, $W_R$
Output: $T_{order}$
for $i = 1$ to $T_{array}$ do
    $P(i)$ = ParaSweep($T_{array}(i)$, $W_R$)
    $P_{high}$ = $P_T + P_T \cdot var$
    $P_{low}$ = $P_T - P_T \cdot var$
    $W_{i_{EZ}}$ = $T_i$ sizes producing performance in range($P_{high}$, $P_{low}$)
    $W_{i_{obfus}}$ = $W_R$ - $W_{i_{EZ}}$
    $Response$ = VertCat($T_{array}(i)$, $W_{i_{obfus}}$)
$R_{order}$ = DecreasingOrder($Response$, $W_{obfus}$)
$T_{order}$ = $R_{order}(Column1)$
return $T_{order}$
```

A. Selection of Transistor(s) to Obfuscate

The primary objectives when selecting transistors to obfuscate are to 1) determine the transistor(s) that provide the smallest range of dimensions that produce circuit performances close to the target performance and 2) ensure a wider range of *obfuscation transistor* sizes. To select the transistor(s) to obfuscate, the target performance parameters are varied by a user-specified percentage, and the range of transistor sizes that produce performance values within the computed performance range, given by W_{EZ} in Algorithm 1, is determined. The W_{EZ} range is subtracted from the permissible range of transistor sizes to determine the obfuscation transistor range, W_{obfus}. The transistor having the largest W_{obfus} range is selected for obfuscation. The selection process continues with the transistor with the next largest W_{obfus} range and proceeds until the requisite number of key bits for the circuit is met. From the results shown in Fig. 4, transistors M_{11} and M_{12} produce obfuscation ranges W_{obfus} of 4.67 µm and 10.7 µm, respectively, for ±5% variation in the target center frequency F_c, which indicates that transistor M_{12} is better suited for obfuscation and is, therefore, more effective in masking the F_c of the BPF.

To reduce the time and design complexity of determining the transistor(s) to obfuscate, an algorithm is developed that outputs an array of transistors in descending order of the transistor obfuscation range W_{obfus}. The pseudocode for the selection of the transistor(s) for obfuscation is provided as Algorithm 1. The inputs to the algorithm include the list of all transistors of an analog circuit whose order must be determined (T_{array}), the target performance parameter(s) P_T, the variation in the performance value(s) *var*, and the allowed parametric range W_R of the sizes of transistors of T_{array}. Based on the inputs, the algorithm begins by selecting a single transistor $T_{\mathrm{array}}(i)$ from T_{array}. The size of $T_{\mathrm{array}}(i)$ is varied in the range W_R, and the performance of the analog circuit $P(i)$ is determined. The range of the *performance exclusion zone* (P_{high}, P_{low}) is computed, and the range of $T_{\mathrm{array}}(i)$ sizes that produce performances that fall between P_{high} and P_{low} is determined and is defined as the transistor exclusion range $W_{i_{\mathrm{EZ}}}$. The transistor obfuscation range $W_{i_{\mathrm{obfus}}}$ is computed by subtracting the transistor exclusion range $W_{i_{\mathrm{EZ}}}$ from the parametric sweep range W_R. The obfuscation range for all transistors in T_{array} is computed. The transistors are arranged in decreasing order of the computed obfuscation range (T_{order}). The algorithm returns the list of the best transistor(s) to obfuscate, T_{order}, that effectively mask the performance(s) of the analog circuit.

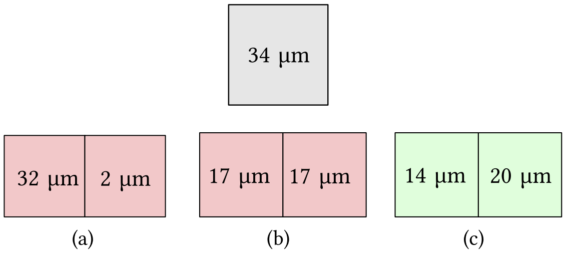


Fig. 6. Three potential subdivisions of a 34 µm target width into two subtarget transistor widths are shown. Both (a) and (b) violate criterion (1), whereas (c) meets the conditions set by criterion (1).

From the determined T_{order}, additional design constraints, including other performance parameters and signal integrity requirements, are applied to further guide the selection of transistor(s) to obfuscate. Obfuscation of the input and output transistors is avoided as adding *obfuscation transistors* along with the corresponding key-delivery circuit directly to nodes tied to inputs and outputs affects the signal integrity. Obfuscating the transistors used for voltage biasing to compensate for the drift in the performance of the circuit due to the implementation of the obfuscation technique results in a less complex tuning of the circuit post-fabrication as compared to obfuscating transistors used for current biasing. Tuning only the applied gate voltage is sufficient to achieve the target circuit performances when obfuscating transistors that set the voltage bias of the circuit, whereas the transistor sizes, currents, and small-signal parameters are modified when obfuscating transistors that set the current bias. Based on the number of transistors to obfuscate (key size), the area, the performance parameters to obfuscate, and any additional design constraints, the designer selects the best suited transistor(s) from T_{order}.

B. Selection of Target Transistor Sizes

Once the transistor to obfuscate is determined, the next step is to ascertain the target transistor sizes. The importance of ensuring proper subdivision of the size of each target transistor is shown in Fig. 6. The goal is to subdivide a 34 µm target width into two sub-transistor sizes while ensuring that only one combination of sub-widths results in the target width. The objective for the remaining combinations of the widths (non-target) is to differ by at least 10% from the target width, where ±10% of 34 µm is 30.6 µm and 37.4 µm. For the combination of widths shown in Fig. 6(a), two key sequences, “11” and “10,” result in effective widths of 32 µm and 34 µm, respectively, which fall within ±10% of the target width of 34 µm. The subdivided target widths shown in Fig. 6(b) are also undesired as multiple key combinations (“10” and “01”) result in redundant effective transistor widths of 17 µm. The subdivision of the target width shown in Fig. 6(c) satisfies both design criteria and provides the correct total width.

C. Selection of Obfuscation Transistor Sizes

The selection of the sizes of the obfuscation transistor(s) is depicted through the example dimensions provided in Fig. 7.

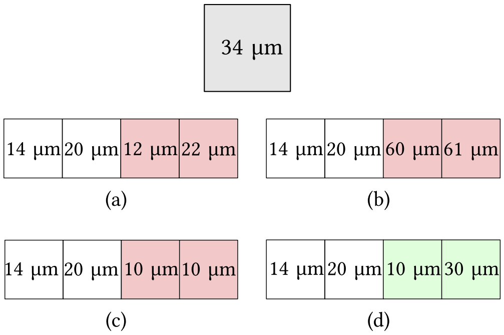


Fig. 7. Consideration of selection criteria when sizing the *obfuscation transistors* for *target transistor* sizes of 14 μm and 20 μm, where the cumulative *target transistor* width is 34 μm. The four scenarios describe (a) when more than one effective width combination is within ±10% of the target width, (b) large difference between the *target transistor* widths and the *obfuscation transistor* widths, (c) presence of redundant widths, and (d) desired *obfuscation transistor* widths that meet all design criteria.

For the widths shown in Fig. 7(a), two keys, "1100" and "0011," result in an effective transistor width of 34 μm. In addition, keys "1001" and "0110" result in effective transistor widths that are within ±10% of the target width of 34 μm, which fails to meet the target design constraint that restricts the sizing of the transistors from producing multiple legitimate values. For Fig. 7(b), the size of the obfuscation transistors shown in red is significantly larger than the target transistor sizes. To minimize the leakage of information, the sizes of the obfuscation transistors must be set to values similar to those of the target transistor sizes while still ensuring the presence of a single correct key, and the application of any incorrect key results in significant degradation in the circuit performances. When both the target and obfuscation transistors are close in size, subtle differences in the circuit performances are observed, which prevents an attacker from eliminating a large portion of the key space. When the obfuscation transistor sizes are either too large or too small as compared to the sizes of the target transistors, the disparity in the output performances is large and more readily observable. Therefore, an attacker must analyze the performances of the circuit for only two transistor sizes, the largest effective transistor size from the smaller range and the smallest effective transistor size from the larger range. The analysis generates two performance values, one closer to the target and the other significantly different. Due to the large disparity, the attacker eliminates the entire range of transistor sizes from which the selected transistor size resulted in a large difference in the performance values, thereby significantly reducing the key/search space.

The selection of redundant dimensions for the obfuscation transistors, as shown in Fig. 7(c), leads to redundant keys that further reduce the key space. The sizes selected for the obfuscation transistors shown in Fig. 7(d) meet all design criteria and are also close to the target transistor sizes, which effectively masks the composite transistor width.

The computational resources needed to solve for the dimensions of the target transistors and the sizing of the obfuscation transistors increase exponentially with key size (2^n for an n-bit key), which results in a lengthy and potentially expensive design cost. An SMT-based algorithm is, therefore, developed, which reduces the overall time needed to select the dimensions of both the *target transistors* and the *obfuscation transistors*. The proposed SMT algorithm reduces the computational complexity while ensuring that 1) the computed transistor sizes produce a single unique key and 2) the closest circuit response due to an incorrect key results in performances that are at least a set percentage away from the specified values.

VI. Analog Satisfiability Algorithm for Transistor Sizing

An SMT-based algorithm is developed that efficiently determines the sizes of the obfuscation transistors that meet the given circuit constraints and obfuscation criteria. The algorithm is executed with the iSAT3 SMT solver [19]. Based on the key size, type of obfuscation (vector- or mesh-based), and range of permissible transistor sizes, an SMT problem is formulated that accounts for the transistor topologies described in Sections IV-A and IV-B. The constraints provided to the SMT algorithm limit the number of effective cumulative widths that are possible around the target width.

A. SMT Problem Formulation

For the vector-based obfuscation technique implemented with an n-bit key, (2) is modified as given by (7) to match the format required by the SMT solver. The problem is formulated as a two-step procedure. The execution of the first step determines the set of all possible combinations of the effective transistor sizes, $S_{T_{\text{eff}}}$, for 2^n key combinations, as given by

$$S_{T_{\text{eff}}} = \left\{T_{\text{eff}_1}, T_{\text{eff}_2}, T_{\text{eff}_3}, \ldots, T_{\text{eff}_{2^n}}\right\}, \quad \text{for} \qquad T_{\text{eff}} = \overrightarrow{T} \cdot \overrightarrow{K}^T \quad \text{and} \quad \forall \overrightarrow{K} \in \{0, 1\}^n, \tag{7}$$

where T_{eff} defines the effective transistor width for a given key sequence $\overrightarrow{K}$ computed using (2). In the second step, the target transistor(s) that produce the desired cumulative width T^*_{eff} are selected. Constraints are added to ensure that only one correct key is produced and any incorrect key results in at least a target percentage variation in performance from the circuit specifications when setting the remaining effective transistor widths. The SMT problem is formulated as

$$\begin{aligned} \phi_{\text{vector}} = {} & T^*_{\text{eff}} \\ & \wedge \left(T_{\text{eff}_1} \leq Width_{\min} \vee T_{\text{eff}_1} \geq Width_{\max}\right) \\ & \wedge \left(T_{\text{eff}_2} \leq Width_{\min} \vee T_{\text{eff}_2} \geq Width_{\max}\right) \\ & \wedge \ldots\ldots. \\ & \wedge \left(T_{\text{eff}_{2^n}} \leq Width_{\min} \vee T_{\text{eff}_{2^n}} \geq Width_{\max}\right), \end{aligned} \tag{8}$$

where ϕ_{vector} defines the problem as provided to the solver, T^*_{eff} is the effective transistor width of the target transistors, and $Width_{\min}$ and $Width_{\max}$ represent the lower and upper bounds of the desired range of widths, respectively.

The range of the desired widths is a user-defined parameter that is set based on two primary constraints: 1) the tuning range of the bias voltages and currents of the analog circuit to compensate for the effects of parasitics, PVT variation, and aging and 2) the desired variation in the target performance of the circuit due to changes to the transistor widths. The consideration of PVT variations during the design phase of the circuit accounts for the required post-silicon margins, which must be considered to meet the target design criteria when sizing the target and obfuscation transistors. Limiting the total acceptable variation ensures that the target transistor sizes are close to the obfuscation transistor sizes, which reduces the amount of leaked information on the sizes of the target transistors.

The steps involved in formulating the transistor sizing problem for the mesh-based obfuscation technique with an $m \cdot n$ bit key are similar to that of the vector-based obfuscation technique. The set of effective transistor widths T_{eff} for the mesh-based technique is calculated using (5), which is modified to the SMT format as

$$S_{T_{\text{eff}}} = \left\{T_{\text{eff}_1}, T_{\text{eff}_2}, T_{\text{eff}_3}, \ldots, T_{\text{eff}_{2^{m \cdot n}}}\right\},$$

where

$$T_{\text{eff}} = \sum_{i=1}^{m}\left(\frac{1}{\overrightarrow{T_i} \cdot \overrightarrow{K}^T}\right) \quad \text{and} \quad \forall \overrightarrow{K} \in \{0,1\}^n. \tag{9}$$

The formulated SMT problem for the mesh-based technique, including the constraint that restricts the number of correct keys and the constraint that results in at least a target percentage variation in the performance specifications due to an incorrect key, is similar to (8) and is given by

$$\begin{aligned} \phi_{\text{mesh}} = \; & T^*_{\text{eff}} \\ & \wedge \left(T_{\text{eff}_1} \le Width_{\min} \vee T_{\text{eff}_1} \ge Width_{\max}\right) \\ & \wedge \left(T_{\text{eff}_2} \le Width_{\min} \vee T_{\text{eff}_2} \ge Width_{\max}\right) \\ & \wedge \ldots\ldots. \\ & \wedge \left(T_{\text{eff}_{2^{m \cdot n}-1}} \le Width_{\min} \vee T_{\text{eff}_{2^{m \cdot n}-1}} \ge Width_{\max}\right). \end{aligned} \tag{10}$$

B. SMT Algorithm

The pseudocode of the algorithm to determine the sizes of the *obfuscation transistors* in a topology that consists of two rows ($i = 2$) after applying mesh-based obfuscation is provided as Algorithm 2, where ϕ defines the SMT formulated problem, as given by (10), and is provided as input to the SMT solver. The algorithm is similar for the vector-based technique; however, ϕ is now given by (8). The SMT solver begins by selecting a random obfuscated transistor in the vector or mesh and splitting the range of dimensions into two subintervals of equal length. The solver then temporarily discards one of the subintervals and reduces the selected interval. The interval constraint propagation (ICP) technique is then applied to ϕ, where the ICP technique determines whether only one target size exists in the *EffectiveWidth* parameter. All other transistor combinations produce sizes that are smaller or larger than a user defined percentage of the target transistor dimensions, which is set to ±10% of the transistor size in this article, as described in Section V. If the ICP routine terminates with no conflict, then the algorithm returns to the decision step and selects a different obfuscation transistor until all transistor sizes in the vector or mesh are set. If a conflict exists, as indicated by a reduction to null of the range of sizes of the given obfuscation transistor, the source of the decision that leads to the conflict is located by a conflict-driven clause learning (CDCL) algorithm. When the union of sources that result in conflict covers the entire search space, the algorithm returns UNSAT. Otherwise, a backtrack routine is called, and the algorithm returns to the decision process after adding a conflict clause to ϕ. The union of all intervals is the superset of the solution space.

VII. Circuit Implementation

The proposed parameter obfuscation techniques are implemented on an active BPF and an op-amp. The selection algorithm is used to determine the transistor(s) to obfuscate, while the SMT algorithm is executed to determine the sizes of the *target transistors* and *obfuscation transistors*. The circuits are designed in a 180 nm technology using Cadence Virtuoso, where the performance analysis is completed using Spectre.

Algorithm 2 aSAT for Obfuscation Transistor Size Optimization for a $2 \times N$ Mesh

```
Input: circuit constraint formulae $\phi$
Output: S
S=empty set
while unassigned ObfusTran with interval greater than $\delta$ exists do
    decision ()
        assign ObfusTran to the mesh and divide the range in half
        select one of the subintervals
    deduction ()
        CombFirst=combination($1^{st}$ row mesh values)
        SumFirst=sum(CombFirst)
        CombSec=combination($2^{nd}$ row mesh values)
        SumSecond=sum(CombSec)
        EffectiveWidth=apply (4)
        if $ICP(\phi)$=UNSAT then
            find conflict-source s
            $S = S \cup s$
            if S=entire state space then
                return UNSAT
            else
                undo all decision and deduction after s
                $\phi$=$\phi \cap \overline{s}$
            end if
    end if
end while
return UNSAT
```

A. Active Inductor-Based Second-Order Band Pass Filter

The schematic of a second-order BPF is shown in Fig. 3. The BPF is composed of two resonator circuits that consist of capacitor C and two active inductors implemented by transistors M_1, M_2, M_5, M_6 and M_3, M_4, M_7, M_8. Input matching is achieved through resistor R_{in} and a common gate transistor M_{in}. The source follower topology that consists of transistor M_{out} and resistor R_{out} forms the output matching circuit. Transistors M_9 to M_{14} implement current sources.

The BPF is designed to operate with a center frequency F_c of 3 GHz, a maximum gain of 30 dB, and a bandwidth (BW) of 500 MHz. The parameter obfuscation technique is applied to mask the gain and the center frequency of the BPF. From the execution of the algorithm that selects the transistor(s) to obfuscate, M_{12} was determined to mask the center frequency F_c, while transistors M_{13} and M_{14} were determined to mask the gain A_v of the BPF. The variation in the center frequency F_c and the gain A_v of the BPF as a function of the width of transistor M_{12} and transistor M_{14} is shown in Figs. 8 and 9, respectively. The size of transistor M_{13} has the same effect on the gain A_v of the BPF as does the size of transistor M_{14}. Therefore, both M_{13} and M_{14} are obfuscated to mask the gain of the BPF.

Transistors M_{12} to M_{14} of the BPF are obfuscated using both the vector- and mesh-based techniques. The schematic representation of the key delivery circuit is shown in Fig. 10,

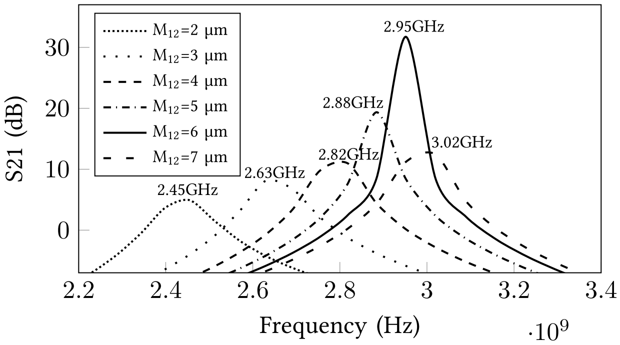


Fig. 8. Variation in the center frequency of the BPF for different currents through transistor M_{12}. An ac input signal of 1 mV is applied to determine the gain.

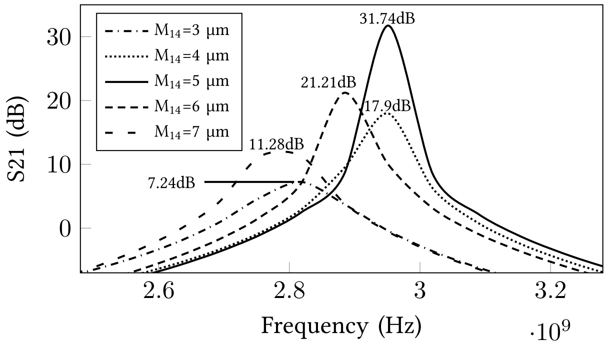


Fig. 9. Variation in the gain of the BPF for different widths of transistor M_{14}. An ac input signal of 1 mV is applied to determine the gain.

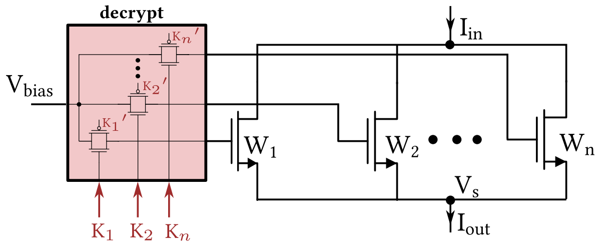


Fig. 10. Schematic of the key-delivery circuit that activates or deactivates the parameter obfuscation transistors based on the applied key bits.

TABLE II

CHARACTERIZATION OF THE CENTER FREQUENCY, GAIN, BW, AND AREA OF A BPF AFTER IMPLEMENTING VECTOR- AND MESH-BASED OBFUSCATION. AN UNOBFUSCATED BPF IS ALSO CHARACTERIZED FOR COMPARISON

Parameter	Unobfuscated	Vector-based	Mesh-based
Center Frequency (F_c)	2.95 GHz	3.02GHz	2.88GHz
Gain (A_v)	31.74dB	31.98dB	33.31dB
3-dB Bandwidth	17.4 MHz	12 MHz	11.2 MHz
Area	11µm^2	24.35µm^2	26.91µm^2

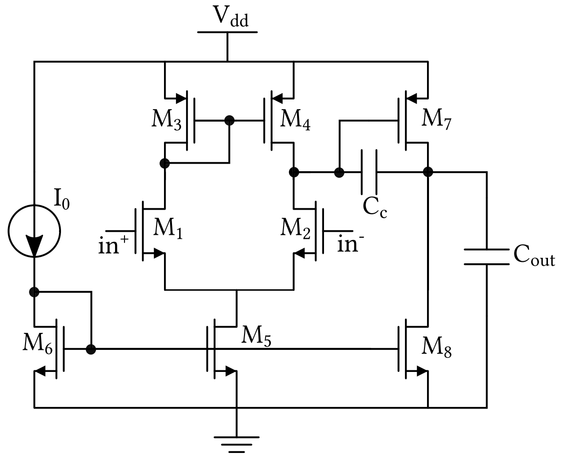


Fig. 11. Circuit schematic of a two-stage op-amp.

where the activation of the transistors is controlled by an applied gate voltage through a decrypt circuit. For key bits that are set to logic high, V_{bias} is applied to the gate of the corresponding *obfuscation* or *target* transistor. When the key bit is set to logic low, the corresponding transistor is off, and no current flows. The total current (I_{in} or I_{out}) is equal to the sum of the currents through the activated paths.

For both the vector- and mesh-based obfuscations of the BPF, transistors M_{12}, M_{13}, and M_{14} are each obfuscated with a 4-bit key, which results in a total key length of 12 bits. The attacker now has to determine the correct gain and center frequency to completely reverse engineer the BPF. The comparisons of the critical parameters of an unobfuscated and obfuscated BPF are listed in Table II.

Due to the additional obfuscation transistors and key decryption circuit, deviation in the performance of the BPF is observed. The performance parameters of the re-tuned obfuscated circuit match closely with the unobfuscated circuit, with results indicating no more than 2.3% deviation in the center frequency F_c and no loss in the gain A_v. However, the area of the BPF increases by 2.2× and 2.7× when implementing the vector- and mesh-based obfuscation techniques, respectively.

B. Operational Amplifier

A two-stage op-amp with a topology as shown in Fig. 11 is considered. The first stage consists of a differential amplifier implemented by transistors M_1 to M_6, while the second stage consists of a common source amplifier implemented by transistors M_7 and M_8. The load capacitance C_{out} is set to 10 fF, and the input common-mode voltage range is set between 0.8 V and 1.6 V. The op-amp is designed to operate with a gain of 60 dB, unity gain bandwith (GBW) greater than 20 MHz, and power dissipation of less than 1 mW.

The parameter obfuscation techniques are implemented on the first and second stages of the op-amp to mask the total gain and the GBW. From the execution of Algorithm 1, which selects transistor(s) to obfuscate, M_5 and M_8 were determined best suited to mask the gain of the amplifier. The change in the gain of the op-amp, defined by the S_{21} parameter as a function of frequency for a peak-to-peak AC input signal of 1 mV, is shown in Figs. 12 and 13 for different widths of transistors M_5 and M_8, respectively. Only when the sizes of transistors M_5 and M_8 are set to 5.25 µm and 35 µm, respectively, is the maximum gain of approximately 63 dB achieved, while the remaining widths produce gains of less than 40 dB.

The op-amp is obfuscated using both the vector- and mesh-based techniques, where transistors M_5 and M_8 are each obfuscated with a 5 bit key (total key size of 10 bits). For the mesh-based obfuscation of transistors M_5 and M_8, two rows are included, where the first row implements 3 bits of the key and the second row the remaining 2 bits. Utilizing Algorithm 2, the sizes of the obfuscation transistors are

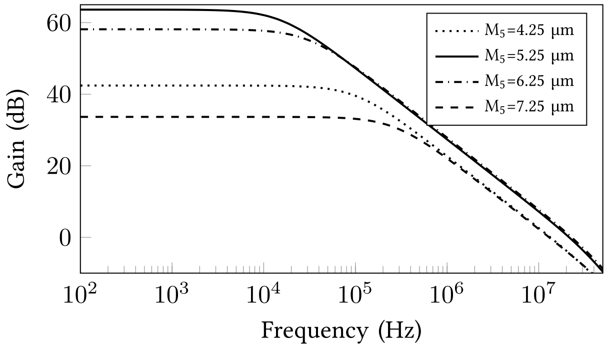


Fig. 12. Variation in the gain of the op-amp for different widths of transistor M_5. An ac input signal of 1 mV is applied to determine the gain.

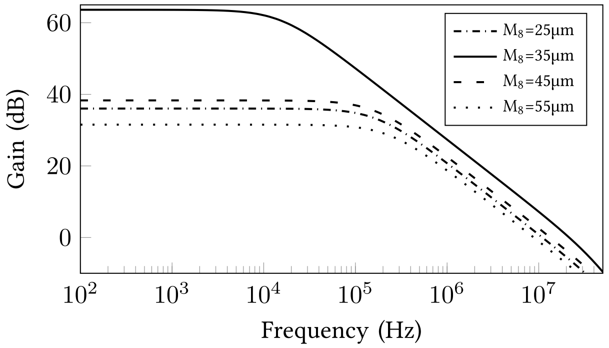


Fig. 13. Variation in the gain of the op-amp for different widths of transistor M_8. An ac input signal of 1 mV is applied to determine the gain.

TABLE III

CHARACTERIZATION OF CRITICAL CIRCUIT PARAMETERS OF AN OP-AMP AFTER APPLYING THE VECTOR- AND MESH-BASED OBFUSCATION TECHNIQUES. THE RESULTS ARE COMPARED WITH AN UNOBFUSCATED OP-AMP

Parameter	Unobfuscated	Vector-based	Mesh-based
A_v	63.6 dB	63.8 dB	64.0 dB
GBW	21.6 MHz	21.3 MHz	21.4 MHz
3-dB BW	15.4 KHz	14.7 KHz	15.3 KHz
Power Dissipation (μW)	330 μW	337 μW	350 μW
Area	213.25 μm^2	334.75 μm^2	477.57 μm^2

determined such that only the correct key produces a gain of 63.6 dB and any incorrect key results in at least a 30% degradation in the gain of the op-amp, which is achieved by sizing the obfuscation transistors of M_5 and M_8 to be at least 40% and 30% shifted from the correct target dimensions, respectively. The results from the characterization of the gain, GBW, 3-dB BW, power dissipation, and area of an obfuscated and unobfuscated op-amp are listed in Table III and indicate that there is a maximum deviation of 0.4 dB in the gain and 0.3 MHz in the unity GBW. However, due to the additional obfuscation circuitry, there is a 1.57× and 2.24× increase in the area of the op-amp after implementing the vector- and mesh-based obfuscation techniques, respectively.

VIII. SIMULATION-BASED MULTIVARIATE BIAS TUNING

To mitigate the drift in the performance of an analog circuit from target values due to the implementation of the obfuscation technique, process variation, and aging, a simulation-based multivariate optimization methodology is developed to tune the body voltage of the transistors and/or the biasing voltages and currents of the circuit. Simulated annealing (SA) is applied in conjunction with SPICE simulation of the circuit in an iterative optimization loop. Optimal bias voltages, bias currents, and body voltages $\overrightarrow{B} = \{B_1, B_2, B_3, \ldots, B_k\}$ are determined through the optimization algorithm, and a cost function (CF) Φ is evaluated from results produced through SPICE simulation. Execution of the SPICE-based simulation loop returns performance values $\overrightarrow{P} = \{P_1, P_2, P_3, \ldots, P_l\}$ that are used to calculate Φ. Φ is computed as a minimization of the difference between the simulated performance $\overrightarrow{P}_{\text{simulated}}$ and the target performance $\overrightarrow{P}_{\text{target}}$ of the circuit.

Algorithm 3 SA Algorithm That Tunes the Bias Voltage and Body Voltage to Properly Calibrate the Performances of an Analog Circuit

```
Input: $P_{target}$, $M$, $N$ $T$, $\alpha$, circuit
Output: $B_{best}$
$B_{current}$ = $Rand()$
$CF_{current} \leftarrow Calculate(B_{current}, circuit)$
$CF_{best}$ = $CF_{current}$
$B_{best}$ = $B_{current}$
for $i$ to $M$ do
    $T_{current} \leftarrow T$
    for $j$ to $N$ do
        $B_j \leftarrow$ SelectBestNeighbor$(B_{current}, circuit)$
        $CF_j \leftarrow Calculate(B_j, circuit)$
        if $CF_j \leq CF_{best}$ then
            $B_{current} \leftarrow B_j$
            if $CF_i \leq CF_{best}$ then
                $B_{best} \leftarrow B_j$
        else if $Formula > Rand()$ then
            $B_{current} \leftarrow B_j$
    $T_{current}$ = $T_{current} \cdot \alpha$
return $B_{best}$
Function Calculate$(B, circuit)$
    $sch \leftarrow schematic(circuit)$
    $net \leftarrow netlist(sch)$
    $\overrightarrow{P}_{simulated}$ = $SpiceSimulation(B, net)$
    CF = $\Phi$ = $|\overrightarrow{P}_{target} - \overrightarrow{P}_{simulated}|$
    return $CF$
```

The pseudocode of the SA-based optimization routine is provided as Algorithm 3. The input to the algorithm includes the target performance values $\overrightarrow{P}_{\text{target}}$, the initial temperature T, the number of times the temperature is decreased M, the number of neighbors searched around a candidate point N, the cooling rate α, and the circuit netlist (circuit). Based on the random initial values of $\overrightarrow{B}$ and T, an initial solution $\overrightarrow{P}$ is determined, and the cost function $\text{CF}_{\text{current}}$ is calculated. Next, a set of N random points in the search space that are slightly modified from the current values of $\overrightarrow{B}$ are explored, and the cost function for each point is computed. If the explored solution results in a lower cost function than the current solution (minimization problem) or if, on calculation of (11), the acceptance probability F is greater than that of a randomly

TABLE IV

RESULTS OF APPLYING THE SIMULATION-BASED OPTIMIZATION ALGORITHM THAT TUNES THE BIASING CONDITIONS AND BODY VOLTAGES OF A BPF AND OP-AMP TO MITIGATE PARASITIC AND PROCESS VARIATIONS WHEN APPLYING VECTOR- AND MESH-BASED OBFUSCATION

Circuit	Parameter		Unobfuscated					Vector-based Obfuscation					Mesh-based Obfuscation				
			TT	FS	SF	SS	FF	TT	FS	SF	SS	FF	TT	FS	SF	SS	FF
BPF	Tuning Parameter	Vb (V)	1	1	1	1	0.74	1	0.9	0.8	0.8	1.05	1	0.75	0.94	1	1
		V_{b1} (V)	1	1	1	1	0.76	1	1	1	0.8	1	1	1	1	1	1
		V_{g1} (V)	0.6	0.56	0.64	0.63	0.51	0.68	0.6	0.72	0.67	0.57	0.66	0.66	0.72	0.57	0.59
		V_{g2} (V)	0.6	0.59	0.65	0.76	0.7	0.7	0.73	0.78	0.8	0.64	0.7	0.62	0.74	0.72	0.61
		V_{g3} (V)	1.2	1.15	1.16	1.06	1.04	1.03	1.03	1.06	1.18	1.12	1.09	1.03	1.06	1.03	1.18
		V_{T_p} (V)	1.8	1.8	1.8	1.5	1.8	1.8	1.8	1.7	1.8	1.8	1.8	1.8	1.8	1.8	1.8
		V_{T_n} (V)	0	0	0	0	0	0	0	0.2	0	0	0	0	0	0.1	0
	Performance Parameter	A_v (dB)	31.74	29.0	30.86	30.55	31.07	31.2	29.2	29.12	32.0	29.0	32.3	28.2	29.8	29.55	30.97
		A_v Error (dB)	0	2.74	0.88	0.89	0.67	0.54	2.54	2.64	0.26	2.74	0.56	2.24	1.94	2.19	0.77
		F_c (GHz)	2.95	3.01	3.09	2.95	3.02	3.02	2.95	3.1	2.9	3.09	2.9	2.95	3.09	2.95	2.95
		F_v Error (%)	0	2.03	4.75	0	2.3	2.37	0	5.08	1.69	4.75	1.69	4.75	4.74	0	0
Op-Amp	Tuning Parameter	I0 (uA)	20	20	20	20	20	19	20	22	22	18	20	20	24	20	20
		VTp (V)	1.8	1.4	1.8	1.7	1.8	1.8	1.6	1.8	1.8	1.7	1.8	1.8	1.7	1.8	1.8
		VTn (V)	0	0	0.4	0	0	0	0	0	0	0	0.5	0	0.5	0.5	0.6
	Performance Parameter	A_v (dB)	63.6	64.1	63.7	63.8	63.5	63.8	63.4	63.9	63.3	64.3	64.0	64.9	64.0	63.4	63.1
		A_v Error (dB)	0	0.5	0.1	0.2	0.1	0.2	0.2	0.3	0.3	0.7	0.4	1.3	0.4	0.2	0.5
		UBW (MHz)	21.6	21.9	22.9	21.9	21.1	21.3	22.3	22.2	21.5	22.5	21.4	21.6	23.8	21.1	22.8
		UBW Error (MHz)	0	0.3	1.3	0.3	0.5	0.3	0.7	0.6	0.1	0.9	0.2	0	1.7	0.5	1.2
		3-dB BW (kHz)	15.4	16.2	14.6	16.9	14.1	14.7	16.3	15.7	16.5	15.7	15.3	14.8	16.7	15.8	16.4
		3-dB BW Error (kHz)	0	0.8	0.8	1.5	1.3	0.7	0.9	0.3	1.1	0.3	0.1	0.6	1.3	0.4	1

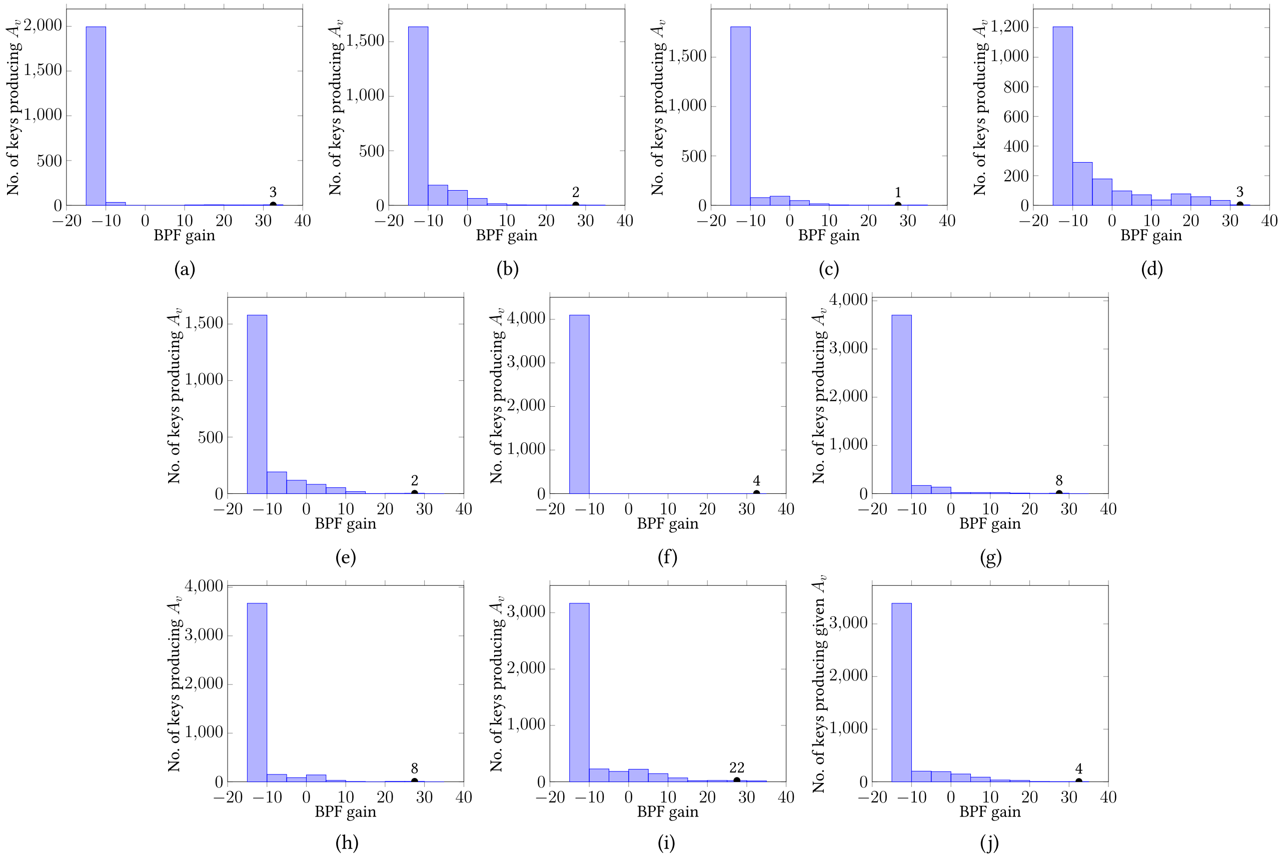
selected point, then a decision to consider the selected solution is made. The temperature T is decreased at a rate α after each iterative selection of N points for M number of iterations, which results in a total of $M \times N$ number of iterations. The algorithm returns the best determined values of the biasing voltages, biasing currents, and body voltages ($\overrightarrow{B}_{\text{best}}$) that produce the lowest cost function CF_{best}, which indicates circuit performance parameters close to the target values.

$$F = \frac{1}{e^{\frac{\text{CF}_{\text{current}} - \text{CF}_i}{T}}}. \tag{11}$$

The simulation-based optimization algorithm is applied to both an obfuscated BPF and an obfuscated op-amp, where the target circuit specifications are met after tuning the biasing points post-obfuscation. In addition, the optimization technique is applied, and the circuit is analyzed to determine the body voltages and biasing voltages that result in the target performances at different process corners. For the BPF, nMOS transistors M_1 to M_4 and pMOS transistors M_5 to M_8 are grouped into two separate domains of body voltages. The two body voltage domains, V_{T_p} and V_{T_n}, as well as the biasing voltages V_b, V_{b1}, V_{g1}, V_{g2}, and V_{g3}, are determined and set using the simulation-based optimization algorithm. The CF of the BPF is such that the sum of the error between the target and simulated gain A_v and center frequency F_c are minimized.

For the op-amp, the simulation-based optimization algorithm is applied to tune the bias current I_0 and the body voltages V_{T_p} and V_{T_n} such that the gain and unity GBW match the target specifications. The nMOS transistors M_1, M_2, M_5, M_6, and M_8 and pMOS transistors M_3, M_4, and M_7 are grouped and tied to the V_{T_n} and V_{T_p} body voltage domains, respectively. The cost function is computed with the goal of minimizing the error between the target and simulated op-amp gain and unity bandwidth (UBW).

The resulting body voltages, bias voltages, and bias currents after executing the simulation-based optimization algorithm on the BPF and the op-amp are listed in Table IV. The SA algorithm was implemented in Python 2.7.5, and the simulation methodology was executed using the Cadence SKILL and OCEAN scripting languages. The number of iterations of the simulation-optimization loop for the BPF is set to 500, where the temperature is decreased 50 times (M=50) from 1000°C to 0°C at a rate of 15% (α=0.85) per iteration. For each decrease in temperature (M=50 iterations), the ten nearest neighbors are searched (N=10). The bias voltages V_b, V_{b1}, V_{g1}, V_{g2}, and V_{g3} are set in the range of 0.4 V to 1.2 V. The tunable range of the pMOS body voltage V_{Tp} is between 1.1 V to 1.8 V, while the nMOS body voltage V_{Tn} is tuned in the range of 0 V to 0.6 V. To prevent latchup, the substrate current is analyzed by varying the body voltage for fixed gate and source/drain voltages for both the pMOS and nMOS transistors. From the analysis, the substrate current exponentially increases for $V_{\text{Tp}} \leq 1.1$ V and $V_{\text{Tn}} \geq 0.6$ V. Therefore, the lower range of V_{Tp} is set to 1.1 V, while the upper range of V_{Tn} is limited to 0.6 V. The biasing voltages and the body voltages of the BPF are determined by the optimization algorithm for the five process corners (TT, FS, SF, SS, and FF) that account for pMOS and nMOS transistors with typical (T), fast (F), and slow (S) operation and for the case of an unobfuscated, vector obfuscated, and mesh obfuscated BPF, with results as listed in Table IV. The results indicate that there is no more than a 2.75 dB difference in the gain, 4.75% difference in the center frequency, and 10 MHz difference in the 3-dB BW of the obfuscated BPF as compared to the unobfuscated BPF. For the cost function (CF) of the BPF calculated using (11), the critical performance parameters considered include the center frequency F_c and gain A_v. Therefore, the resulting difference between the target and simulated F_c and A_v is weighted by a factor of ten, which results in a greater value in the calculated CF as compared to the value produced by the bandwidth parameter. The optimization algorithm determines the tuning voltages and currents that minimize the error between the target and simulated values of the parameters with the greatest impact on the CF, which, in this case, are the weighted center frequency and gain.



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

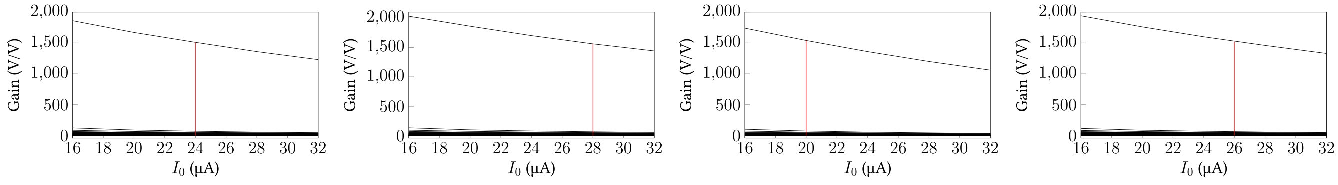
Fig. 14. Histogram of the gain of a BPF for different applied keys, where the gain is in the range of −15 dB to 35 dB. The BPF is obfuscated using the vector- and mesh-based techniques, with analysis performed on the obfuscated BPF for different process corners. Vector-based obfuscation in the (a) TT process corner, (b) FS process corner, (c) SF process corner, (d) SS process corner, and (e) FF process corner. Mesh-based obfuscation in the (f) TT process corner, (g) FS process corner, (h) SF process corner, (i) SS process corner, and (j) FF process corner.

For the op-amp, the number of iterations of the simulation-based optimization loop is set to 70. The optimum biasing current I_0 and the body bias voltages V_{T_p} and V_{T_n} are determined for the five process corners (TT, FS, SF, SS, and FF) and for an unobfuscated, vector obfuscated, and mesh obfuscated op-amp. The temperature is decreased ten times (M=10) from 1000°C to 0°C at a rate of 15% (α=0.85) per iteration, and for each iteration of decreasing temperature, the seven nearest neighbors are searched (N=7). The range of I_0 is set to between 10 μA and 50 μA with a maximum step size of 1 μA. The tunable range of the pMOS body voltage V_{Tp} is set to between 1.1 V and 1.8 V, while the nMOS body voltage V_{Tn} is tuned in the range of 0 V to 0.6 V to prevent latchup. The step size for both V_{Tn} and V_{Tp} is 0.1 V. The results of executing the optimization algorithm on the op-amp are listed in Table IV, where the determined I_0 and body voltages produced no more than a 0.7 dB difference in the gain, 1.7 MHz difference in the unity gain bandwidth, and 1.5 kHz (less than 10%) error in the 3-dB bandwidth as compared to an unobfuscated op-amp.

A. Considering Parameter Tuning for Variation When Implementing the Obfuscation Techniques

The effect of PVT variations and the implementation of the biasing compensation technique leads to drift in the performance of an analog circuit for a given applied key, which potentially results in the circuit performing close to the target specifications for incorrect keys and the generation of multiple correct keys. To prevent the application of incorrect keys from producing circuit performance values close to the target specifications, an SMT algorithm is developed and executed to size the obfuscation transistors such that any incorrect key results in an adequate difference in the performance parameters from the target values. For the BPF and the op-amp, a 15% difference in the effective transistor widths between the correct and incorrect keys results in at least a 25% error in the gain and 10% error in the center frequency of the BPF and at least a 43.7% error in the gain of the op-amp after applying the obfuscation techniques and characterizing across the five process corners (TT, FS, SF, SS, and FF).

The number of keys that produce a given gain for the BPF after implementing the vector- and mesh-based obfuscation techniques and across different process corners is shown in Fig. 14. The histograms are composed of bins of 5 dB increments that include the subset of keys that produce a given gain in the range of −15 dB to 35 dB. Although a subset of keys exists within the bin containing the correct key, the gain produced by the incorrect keys varies by at least 2.5 dB from the target gain of the BPF for all corners. In addition, the center frequency F_c of the BPF for an incorrect key varies by at least 2.7 MHz (10%) from the target F_c. For the worst case conditions, where the BPF is obfuscated using the mesh-based technique and is characterized in the SS process corner, the number of keys that produce a gain between 25 and 30 dB is 22, as shown in Fig. 14(i). The correct key produces a gain of 29.55 dB (30.02×), while the remaining 21 incorrect keys produce gains that are at least 2.5 dB less than the target gain (27.03 dB or 22.46×), which equates to at least a 25.2%



(a) (b) (c) (d)

Fig. 15. Analysis of the variation in the gain of the op-amp for all 2^{10} effective sizes of M_5 and considering a 25% tuning range of bias current I_0. The analysis is performed in the (a) SS, (b) SF, (c) FS, and (d) FF process corners.

reduction in the maximum gain of the BPF. The closest gain of the BPF closet to the target of 29.55 dB falls within the 30 dB to 35 dB bin, with a value of 33.07 dB (45.03×). The resulting gain is 52.4% (3.52 dB) greater than that of the target value. For a given application, where a BPF is required, gains greater than the target gain result in frequency and phase distortions of the output signal and force one or more transistors to operate in an incorrect region. Similar trends are observed for both the vector- and mesh-based obfuscation techniques and across process corners, which ensures that a unique key produces the target output performances at all corners, while incorrect keys result in a significant difference in the performance of the BPF even when considering process variations.

In addition, the impact of the bias current I_0 on the gain of the op-amp shown in Fig. 11 is analyzed, with the objective being to assure that only the correct key produces the desired gain for all values of I_0 and at all PVT process corners. For the analysis, the size of transistor M_5 is masked with a 10 bit key using the vector-based technique, which obfuscates the gain of the op-amp. The bias current I_0 is varied by ±30% of 24 µA, which was determined for the TT process corner, with the results of sweeping I_0 to tune the gain to 63.6 dB shown in Fig. 15. The results indicate that, when the sizes of the obfuscation transistors are designed properly, the biasing circuit tunes the performance of the op-amp to the target value for only the correct key. For an incorrect key, the bias tuning circuitry is not capable of compensating for the degraded performance of the op-amp at any corner.

The analog circuit is configured with the correct calibration voltages and/or currents only while in the test mode. In most analog circuits, the calibration circuitry is only accessible and configurable during testing and is disabled while in normal operation. Therefore, an attacker possessing the oracle analog IC must enter the test mode to modify the calibration voltages and/or currents. For the assumed threat model, where an attacker is assumed to possess the circuit netlist, the attacker must determine both the effective transistor sizes and the calibration voltages and/or currents, which, therefore, significantly increases the search space. For the BPF, considering both the tuning and obfuscation transistor sizes as unknowns, the total number of unique combinations is approximately 13×10^9.

For circuits where the acceptable performance range is large, obfuscating the calibration circuit provides additional benefits to obfuscating the transistor sizes of the analog circuit. Obfuscating the calibration circuits allows for the minimization of the effects of PVT variation and mismatch when a correct key is applied to ensure that the analog circuit operates within an acceptable performance range. Any incorrect key inaccurately compensates for PVT variations and mismatches and, therefore, results in severe degradation in the performance of the circuit. The flexibility of the proposed technique, including the proposed obfuscation circuit, is not limited to the obfuscation of only the analog circuit blocks but is also applicable to the peripheral biasing and/or calibration circuits.

TABLE V

Analysis of the Security Provided by Analog Obfuscation Techniques to an Untrusted Foundry and an Untrusted End User. The Probability of Determining the Correct Key Is Also Evaluated

Obfuscation Technique	Threat Model		BPF		Op-Amp	
	Untrusted Foundry	Untrusted End-user	No. of Keys	Probability	No. of Keys	Probability
Vector-based	✓	✓	12-bit	$\frac{1}{2^{12}}$	10-bit	$\frac{1}{2^{10}}$
Mesh-based	✓	✓	12-bit	$\frac{1}{2^{12}}$	10-bit	$\frac{1}{2^{10}}$
Current Mirror-based	✓	✓	Not-applicable		10-bit	$\frac{1}{2^{10}}$
Multi-threshold	✗	✓	16-bit	$\frac{1}{3^{16}}$	8-bit	$\frac{1}{3^{8}}$

IX. Metric Evaluating the Security of Analog Obfuscation Techniques

The proposed parameter obfuscation technique is compared with current-mirror based obfuscation [15] and multi-threshold based obfuscation [10]. The threat models considered include an untrusted foundry and an untrusted end user. The attacker is assumed to possess the circuit netlist and has knowledge of the target specifications through a datasheet or an active IC. In addition, access to the key and primary inputs is assumed, through which an attacker is capable of changing the key or primary inputs and observing the corresponding outputs. However, the attacker does not possess advance models or knowledge that facilitates further pruning of the key space. For the given threat model, the attacker is only able to execute a brute-force attack, where the metric to evaluate the security of the obfuscation techniques is the probability of determining the correct key.

The results from the comparison of the three analog obfuscation techniques are listed in Table V, where equal key lengths are applied for parameter obfuscation and for current-mirror based obfuscation. The search space for the multi-threshold based obfuscation technique is given by 3^P, where P is the number of transistors in the circuit. The probability of determining the correct V_T for all transistors is $[1/(3^P)]$. Therefore, even assuming that there are multi-threshold devices available in a given fabrication process, the application of the multi-threshold obfuscation technique is limited to analog circuits where P is large. For the parameter- and current-mirror based obfuscation techniques, the key size and the search space are only limited by a given area overhead. Therefore, a much larger number of combinations of parameter values is possible with a tradeoff in increased area. The multi-threshold obfuscation technique does not protect analog ICs from an untrusted foundry as the V_T information of the transistors is provided to the foundry for fabrication. In addition, the multi-threshold obfuscation technique proposed in [10] does not address the possibility

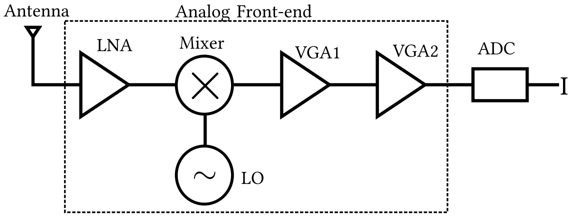


Fig. 16. Block diagram of the direct conversion receiver.

of different V_T transistor combinations producing the target specifications or even specifications that are close enough to the target.

Given the same key size, the probability of determining the correct key for both the parameter- and current-mirror based obfuscation techniques is the same for the op-amp. However, the current-mirror based technique cannot be applied to the BPF as no current mirrors are present in the circuit to obfuscate. In addition, due to key sharing of transistors among the branch currents, the number of combinations is reduced to $2^{\min(\text{branches},\text{keysize})}$ as all the transistors in a given branch must be active for the current to flow through the branch. The vector- and mesh-based obfuscation techniques provide flexibility in the key size, provide security against both an untrusted foundry and an untrusted end user, and can be implemented on any analog circuit topology.

X. Discussion

The primary aim of the developed parameter obfuscation techniques is to thwart analog IP theft by making an attack extremely time-consuming, complex, and expensive. In addition, the resources required to attack the protected analog circuit and determine the key must far outweigh the resources needed to design the analog circuit, which implies a higher cost to reverse engineer and counterfeit a circuit. Implementing the parameter obfuscation techniques increases the time and cost of determining the key. To increase the resilience of the parameter obfuscation techniques to overproduction, body voltages are also obfuscated along with biasing conditions at a cost of added area and complexity. The results listed in Table IV indicate that the biasing voltages of the BPF across fabricated dies vary for different process corners and, therefore, require distinct keys to properly obfuscate the biasing points.

The characterization of the area due to the implementation of the parameter obfuscation techniques is in comparison to an unobfuscated version of the circuit block, which results in a significant increase. However, the percentage of the area when considering the entire analog system or even an entire mixed-signal IC is a fraction of the total. For the direct conversion receiver shown in Fig. 16, which is implemented in a TSMC 65-nm process, the variable gain amplifiers (VGAs) are obfuscated, masking the gain and the center frequency (F_c) of the analog front-end circuit. The receiver is designed to operate in the 2.5 GHz band with 100 MHz channel bandwidth. For an incorrect key, the gain and F_c of the analog front-end signal are degraded, which leads to bit errors in the signal I at the output of the analog-to-digital converter (ADC). Both VGA1 and VGA2 of the receiver are obfuscated with a 10 bit key, which results in a total key length of 20 bits. The total area of the sub-blocks, which includes the area of both active and passive devices, of the obfuscated and unobfuscated receivers is listed in Table VI. The results indicate that, when analyzing only the VGA1 block, the area increases by 4.4× or 342%. However, as compared to the entire analog front-end block, the total area increases by only 0.21%. In addition, for VGA2, which consists of two large metal–insulator–metal (MIM) capacitors, the obfuscation transistors and the corresponding lower metal layer interconnects are placed beneath the MIM capacitors, which results in no increase in the overall area. Furthermore, the key storage and key delivery circuit are integrated with the bias tuning circuit of the receiver, which results in no area penalty for the obfuscated receiver.

TABLE VI
Comparison of the Total Area (Active and Passive) of Subblocks of an Unobfuscated Receiver and a Receiver Obfuscated With a 20-Bit Key

Circuit	Unobfuscated Area	Obfuscated Area	% Area Increase (×area)
VGA1	672 μm^2	2971 μm^2	342% (4.4×)
VGA2	16434 μm^2	16434 μm^2	0% (1×)
Receiver - ADC	1.107044 mm^2	1.109343 mm^2	0.21% (1.002×)
Receiver + ADC	1.22774 mm^2	1.230073 mm^2	0.18% (1.001×)

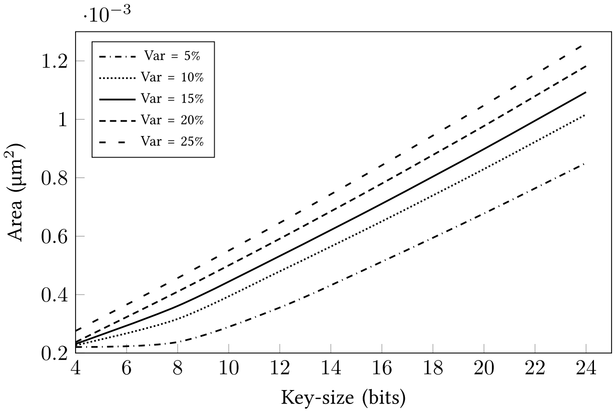


Fig. 17. Relation between the key size and the area of an op-amp obfuscated using the vector-based obfuscation technique for different percentage variation of both the target transistor size and the obfuscation transistor size.

The relation between the key size and the active area of the vector obfuscated op-amp is shown in Fig. 17 for different percentage variation of both the *target transistor* size and the *obfuscation transistor* size. The active area of the analog circuit linearly increases with the key size. In addition, for a fixed key size, the active area of the analog circuit also increases linearly with the percentage variation of both the *target transistor* size and the *obfuscation transistor* size. However, the execution time of the SMT algorithm to determine the sizes of the *obfuscation transistors* increases exponentially with key size, as shown in Fig. 18, since the computational resources needed to solve for the dimensions of the *obfuscation transistors* increase at the rate of 2^n for an n-bit key. In order to reduce the computational time for the same key size, multiple transistors in the analog circuit are obfuscated. For example, the computational complexity for obfuscating a single transistor in an analog circuit secured with a 20 bit key is 2^{20}, whereas the computational complexity is reduced to 2×2^{10} for obfuscating two transistors each with a 10 bit key. In addition, obfuscating multiple transistors has the added advantage of masking multiple performance parameters

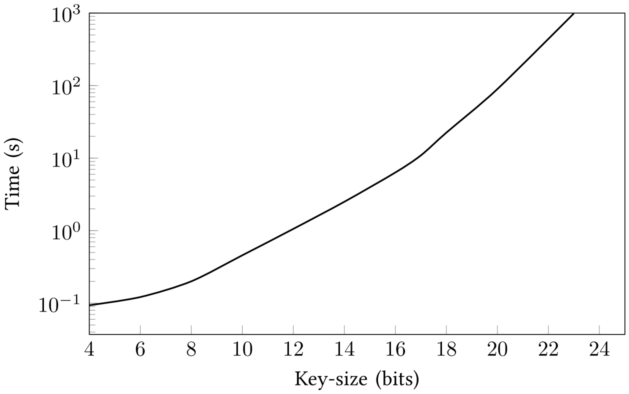


Fig. 18. Relation between key size and the execution time of the SMT algorithm to determine the obfuscation transistor sizes when implementing the vector-based obfuscation technique.

and, along with the key-sharing technique proposed in [20], further increases the security provided by an implemented obfuscation technique.

XI. Conclusion

Parameter obfuscation is proposed to protect analog circuits against IP piracy attacks, including reverse engineering, counterfeiting, and overproduction. Two techniques, vector- and mesh-based obfuscation, are described, which provide a varying degree of security to an analog circuit. The results of implementing the two obfuscation techniques on a BPF and op-amp indicate that the critical circuit performances are properly obfuscated with at least a 15% variation in the properties of the circuit when setting the correct and incorrect transistor sizes. To reduce the complexity of determining the sizes of the obfuscation transistors, an SMT-based algorithm is proposed to search the design space. The effects of parasitic and process variations are mitigated by a simulation-based optimization technique that tunes the biasing conditions (voltages and currents) and the body bias of the transistors to obtain the desired circuit performances. In addition, the SMT and simulation-based transistor ordering and optimization algorithms prove to be efficient in reducing the design time and the number of recycles when implementing the parameter obfuscation techniques on an analog circuit.

References

[1] *Analog Integrated Circuit (IC) Market by 2019 by Type, Application, Provider, Demand Analysis, Emerging Trends and Investment Opportunities to 2024*, Orbis Research, Rahatani, India, Aug. 2016.

[2] *Analog Integrated Circuit (IC) Market 2019—Industry Size, Share, Dynamics, Status, Outlook and Opportunities: 2024*, Analytical Research Cognizance Report, Pune, India, Sep. 2019, pp. 1–120.

[3] *IoT Platforms: Enabling the Internet of Things*, IHS Markit Report, London, U.K., Mar. 2016.

[4] C. Brown and G. Linden, *Chips and Change: How Crisis Reshapes the Semiconductor Industry*. Cambridge, MA, USA: MIT Press, Aug. 2009.

[5] M. M. Alam *et al.*, "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.

[6] *Top 5 Most Counterfeited Parts Represent A 169 Billion Potential Challenge for Global Semiconductor Market*, IHS Technology Press Release, London, U.K., Apr. 2012.

[7] A. Antonopoulos, C. Kapatsori, and Y. Makris, "Security and trust in the analog/mixed-signal/RF domain: A survey and a perspective," in *Proc. 22nd IEEE Eur. Test Symp. (ETS)*, May 2017, pp. 1–10.

[8] Y. Bi, J. S. Yuan, and Y. Jin, "Beyond the interconnections: Split manufacturing in RF designs," *MDPI Electron.*, vol. 4, no. 3, pp. 541–564, 2015.

[9] 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.

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

[11] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans: Extended version," *J. Cryptograph. Eng.*, vol. 4, no. 1, pp. 19–31, Apr. 2014.

[12] T. Sugawara *et al.*, "Reversing stealthy dopant-level circuits," *J. Cryptograph. Eng.*, vol. 5, no. 2, pp. 85–94, Jun. 2015.

[13] V. V. Rao and I. Savidis, "Protecting analog circuits with parameter biasing obfuscation," in *Proc. 18th IEEE Latin Amer. Test Symp. (LATS)*, Mar. 2017, pp. 1–6.

[14] V. V. Rao and I. Savidis, "Mesh based obfuscation of analog circuit properties," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–5.

[15] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu, "Thwarting analog IC piracy via combinational locking," in *Proc. IEEE Int. Test Conf. (ITC)*, Oct. 2017, pp. 1–10.

[16] 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. Int. Conf. Comput.-Aided Design*, Nov. 2018, pp. 1–8.

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

[18] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proc. 48th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2011, pp. 333–338.

[19] K. Scheibler, S. Kupferschmid, and B. Becker, "Recent improvements in the SMT solver ISAT," in *Proc. Methods Description Lang. Modeling Verification Circuits Syst. Conf.*, Mar. 2013, pp. 231–241.

[20] K. Juretus, V. V. Rao, and I. Savidis, "Securing analog mixed-signal integrated circuits through shared dependencies," in *Proc. Great Lakes Symp. VLSI*, May 2019, pp. 483–488.

Vaibhav Venugopal Rao (Student Member, IEEE) received the B.E. degree in electronics and communications from Visvesvaraya Technological University, Belgaum, India, in 2015, and the M.Sc. degree in computer engineering from Drexel University, Philadelphia, PA, USA, in 2017, where he is currently working toward the Ph.D. degree at the Department of Electrical and Computer Engineering.

His current research interests include circuit-level techniques to protect analog IP from intellectual property theft and counterfeiting, and variation-aware automation of analog circuit design to reduce design time.

Ioannis Savidis (Senior Member, IEEE) received the B.S.E. degree in electrical and computer engineering and biomedical engineering from Duke University, Durham, NC, USA, in 2005, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Rochester, Rochester, NY, USA, in 2007 and 2013, respectively.

He joined the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, USA, in 2013, where he is currently an Associate Professor and directs the Integrated Circuits and Electronics (ICE) Design and Analysis Laboratory. His current research interests include analysis, modeling, and design methodologies for high-performance digital and mixed-signal integrated circuits, power management for system-on-chip (SoC) and microprocessor circuits, hardware security, including digital and analog obfuscation and Trojan detection, and electrical and thermal modeling and characterization, signal and power integrity, and power and clock delivery for heterogeneous 2-D and 3-D circuits.

Dr. Savidis is a member of the Association of Computing Machinery, the IEEE Circuits and Systems Society, the IEEE Communications Society, and the IEEE Electron Devices Society. He serves on the organizing committees of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), the ACM Great Lakes Symposium on VLSI (GLSVLSI), and the IEEE International Symposium on Circuits and Systems (ISCAS). He also serves on the Editorial Boards of the IEEE Transactions on Very Large Scale Integration (VLSI) Systems and the *Microelectronics Journal*.