Towards Provably-Secure Analog and Mixed-Signal Locking Against Overproduction

Nithyashankari Gummidipoondi Jayasankaran
Texas A&M University
College Station, Texas
gjn@tamu.edu

Adriana Sanabria Borbon
Texas A&M University
College Station, Texas
adca.sanabria@tamu.edu

Edgar Sanchez-Sinencio
Texas A&M University
College Station, Texas
sanchez@ece.tamu.edu

Jiang Hu
Texas A&M University
College Station, Texas
jianghu@tamu.edu

Jeyavijayan Rajendran
Texas A&M University
College Station, Texas
jv.rajendran@tamu.edu

Abstract

Similar to digital circuits, analog and mixed-signal (AMS) circuits are also susceptible to supply-chain attacks such as piracy, overproduction, and Trojan insertion. However, unlike digital circuits, supply-chain security of AMS circuits is less explored. In this work, we propose to perform "logic locking" on digital section of the AMS circuits. The idea is to make the analog design intentionally suffer from the effects of process variations, which impede the operation of the circuit. Only on applying the correct key, the effect of process variations are mitigated, and the analog circuit performs as desired. We provide the theoretical guarantees of the security of the circuit, and along with simulation results for the band-pass filter, low-noise amplifier, and low-dropout regulator, we also show experimental results of our technique on a band-pass filter.

Keywords

AMS security, logic locking, process variations

ACM Reference Format:
Nithyashankari Gummidipoondi Jayasankaran, Adriana Sanabria Borbon, Edgar Sanchez-Sinencio, Jiang Hu, and Jeyavijayan Rajendran. 2018. Towards Provably-Secure Analog and Mixed-Signal Locking Against Overproduction. In *Proceedings of ICCAD (ICCAD'18).* ACM, San Diego, CA, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

1.1 Motivation

The increasing cost of manufacturing of integrated circuits (IC) has forced many companies to go fabless over the years. With the outsourcing of IC fabrication in a globalized/distributed design flow including multiple (potentially untrusted) entities, the semiconductor industry is facing a number of challenging security threats. This fragility in the face of poor state-of-the-art intellectual property (IP) protection has resulted in hardware security vulnerabilities such as IP piracy, overbuilding, reverse engineering, and hardware Trojans [12]. To address these issues most effectively at the hardware level [8], a number of hardware design-for-trust (DfTr) techniques such as IC metering, watermarking, IC camouflaging, split manufacturing, and logic locking [9, 13, 22, 23, 25] have been proposed. Logic locking, in particular, has received significant interest from the research community, as it can protect against a potential attacker located anywhere in the IC supply chain, whereas other DfTr techniques such as camouflaging or split manufacturing can protect only against a limited set of malicious entities.

Logic locking inserts additional logic into a circuit, locking the original design with a secret key. A locked design produces correct outputs only upon applying the correct key; otherwise incorrect outputs are produced. In addition to the original inputs, a locked circuit has *key inputs* that are driven by an on-chip tamper-proof memory [6, 19], as shown in Fig. 1. In case of digital designs, the additional logic may consist of XOR gates [9, 13] or look-up tables (LUTs) [1]. The locked netlist passes through the untrusted design phases. Without the secret key (i) the design details cannot be recovered (for reverse-engineering), and (ii) the IC produces incorrect outputs (for over-production). A locked IC has to be activated by loading the secret key onto the chip's memory.

While logic locking techniques exist for digital circuits, there is a great dearth of techniques for AMS IP protection. In fact, analog IPs are the most counterfeited semiconductor product and are the weakest link in a complex system, because of the lack of defense techniques [15]. Analog ICs are vulnerable to IP piracy as they have relatively low transistor count and they are often associated with distinct layout patterns, making it easy for a malicious foundry to reverse engineer the layout. Hence, in this work, we develop a defense technique to prevent overproduction of AMS ICs.

1.2 Problem statement

While logic locking schemes are well-defined for digital designs, there is no formal approach for analog designs. In this work, we develop a logic locking scheme for AMS designs. Here, only on applying the correct key, the locked AMS design will produce the desired response. Otherwise, for an incorrect key, the response deviates from the desired value. For example, in the case of band-pass filter (BPF), it exhibits the desired frequency response for correct key and an incorrect frequency response for an incorrect key.

ICCAD'18, Nov 2018, San Diego, CA, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

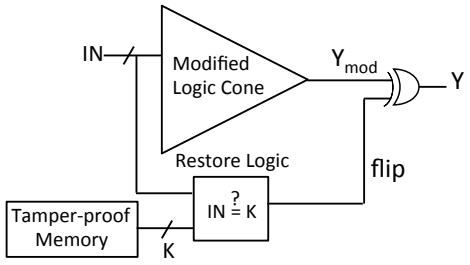

Figure 1: The logic locking technique used in [25]. The logic cone is minimally modified by inverting the response of one input combination w.r.t. original logic cone. The restore logic fixes this inversion for the correct key for the intended input combination and introduces a second inversion for all incorrect keys.

1.3 Prior work on AMS locking

There are very few previous works on the security of AMS designs. A locking technique using memristors is proposed in [4]. It uses a memristor-based voltage divider to bias the body voltage of transistors in an amplifier. The voltage divider output is programmed by a memristor crossbar. The correct voltage output is obtained only when a 16-bit key is inputted to configure the crossbar correctly. This scheme conceptually works well, but its practical applicability is quite restrictive due to its dependence on memristor, and hence it is not applicable to conventional CMOS-based AMS designs. A split manufacturing technique for RF circuits is proposed in [2] for security defense against untrusted foundry. While this technique requires the trusted user, our work technique does not require a trusted end-user.

An SMT-based combinational locking was proposed in [20]. This defense mechanism ensures that each chip has a unique key. Hence any attack to make the chip usable by finding the key is applicable only for that chip. Though this technique has increased the bar of the attack by using SMT-based combinational locking, it has certain disadvantages: (i) Application of incorrect key may sometimes produce close to the desired response, in our work we ensure that the circuit response suffers a deterministic error for an incorrect key. (ii) This work ignores the fact that SAT attack is an oracle guided attack, and hence when this attack is run on an AMS design, the output from the miter circuit can be validated by the output from the Oracle for the same input. Though this locking is vulnerable to SAT attacks, as each chip has a unique key, the attack has to be run on all required chips which are time-consuming. Another work on obfuscating analog circuit performance using locking technique is proposed in [10]. Applying the right key, sets the required transistor width in the current mirror, which in turn provides the suitable bias current for the analog circuit operation. Though this work has shown a simplistic method for analog locking, it has not proved its resilience against SAT attack.

1.4 Challenges in AMS locking

A simple and an obvious approach to lock an AMS design is to insert key-gates into the analog circuit. Such key gates can be realized as transistors, selection of bias voltages, selection of bias currents, etc. But, such simple approach suffers from the following issues:

- As this will include a minimal number of key-transistors, it will be trivial to find the right key inputs by brute forcing and analyzing the output response for each key combinations.
- Owing to the small device count on analog design - which can have only a few hundreds of transistors on a single chip (or even less), it is quite easy to reverse engineer compared to the digital circuits which have millions of transistors on a single chip.
- Once the reverse-engineered netlist is available, the attacker can find the protected parts and remove them, thereby regaining the original circuit [24].

1.5 Proposed approach

Piracy vs. overproduction. In case of analog designs, most of the commonly-used circuits have a standard structure, and are easy to reverse engineer. Also, an attacker can always recreate a design from scratch, given the parametric specification; an attacker can obtain such information from the publicly-available datasheet. These challenges make it difficult to prevent piracy attacks, where the attacker can copy the design, make the masks, and manufacture new chips. Hence, we try to prevent against overproduction, where the foundry uses the masks and makes new chips. Our technique renders the overproduced chips non-functional, even if the attacker has access to the complete specification of the target chip.

Our technique for protecting analog circuit is to logic lock the digital section of AMS circuit that minimizes the effect of process variation by setting the tuning knobs of an analog circuit to their optimal values. Analog circuits are susceptible to process variations; for instance, a filter can suffer up to 20% of variation due to the component's tolerances [18]. Many approaches have been proposed to minimize the effect of process variations [7]. In these efforts, the tuning knobs of analog circuits (e.g., resistances, capacitances) are set to their optimal values; the digital components determine such optimal values. By performing *judicious* logic locking on the digital components of such circuits, only on applying the correct key, the effect of process variations are nullified as the digital circuit works correctly, and thus making the analog circuit to perform as desired. On applying an incorrect key, the digital circuit produces incorrect output, thereby setting the tuning knobs of the analog circuit to non-optimal values. This causes deterioration in the functionality of the analog circuit.

If the logic locking technique is secure, the attacker will not be able to mitigate the effect of process variations without the key. Therefore, all the overproduced chips will be susceptible to process variations. Since process variations have deteriorating effects on AMS circuits, the overproduced chips will not adhere to the specification.

Our approach provides the following benefits:

(1) By setting the default analog operation points to where the harmful process variation effect is amplified, even if the attacker removes the locked digital circuit, the resultant analog circuit will not function as desired, because the amplified harmful effect of process variations stays, thus making the resultant circuit non-functional.
(2) The tuning knobs are selected such that even a small amount of change in their values significantly impact the behavior of analog circuits.
(3) Since we cannot protect all the input patterns of the digital circuits, we protect only those input patterns that significantly impact the values of the tuning knobs, thereby the output of the analog circuit.

(4) Furthermore, we judiciously perform all these steps to minimize area, power, and delay overheads.

1.6 Contributions

The paper has the following contributions:

- The first technique that can protect AMS designs against overproduction, including removal and other attacks.
- A logic locking solution that is applicable to a wide variety of analog circuits like BPF, low-noise amplifier, low-dropout regulators, etc.
- A sensitivity analysis that can maximize the impact of protection, thereby reducing the overhead.
- We demonstrate our technique on three different AMS circuits: BPF, LNA, and LDO, including experimental results from a chip that implements a BPF circuit.

The paper is organized as follows. In Section 2, we explain the background and previous work related to logic locking and process variations impact on AMS circuits. In Section 3, we explain the locking strategy with the BPF circuit as a motivational example. Section 4 shows the experimental and simulation results of the proposed technique. Section 5 concludes the paper.

2 Background

2.1 Logic locking

In this paper, we use the logic locking technique proposed in [25], called stripped-functionality logic locking (SFLL). SFLL modifies the design logic cone to invert its output for a selected (protected) input pattern, as shown in Fig. 1. The modification can be affected via a logic gate insertions/replacements. The desired impact is an inverted output for only one input pattern corresponding to the correct key. The restore unit then inverts the inverted output only for the correct key, thereby restoring the correct output. For any incorrect key, SFLL produces an inverted output for the protected input pattern. Both the key and the protected input pattern are the designer's secrets.

SFLL is provably-secure: it is secure against all attacks—SAT attack [16], removal attack [24], sensitization attack [9], and bypass attack [23]. For a design with an n-bit input, it can only protect $k - \lceil \log_2 \binom{k}{h} \rceil$ out of the 2^n possible input patterns, where k is a pre-defined security level. The security properties hold true only for the input patterns protected. In the context of this proposal, we call these input patterns as malfunction input patterns (MIPs), because they cause analog circuit malfunction. We use two types of SFLL techniques, *HD-0*, and *HD-h*. *HD-0* can protect only one input pattern, and *HD-h* can protect $2^{n-k} \cdot \binom{k}{h}$ patterns, where n is the number of bits in the input design, k is the size of the key, and h is the Hamming distance, a parameter. Proof of security against these attacks are detailed in [25].

Usually, the protected patterns are selected by the designer based on application needs. In the context of this research, one needs to select what input patterns of the optimizer, that eliminates the process variations effects. This way, an incorrect key will not eliminate the effect of process variations.

2.2 Analog ICs and process variations

The performance of analog circuits is degraded by process, voltage, and temperature (PVT) variations. At the design stage, the designer chooses a topology and find the sizes that meet the specifications. After that, aware of the expected variation, the designer use corners, and Monte Carlo analysis to test and improve the robustness of the design. The impact of the performance variation depends on the particular application. However, after fabrication, there is no way to compensate these variations. So, researchers embed a built-in self-test (BIST) and in-situ analog circuit optimization circuit to test and correct the performance on-chip [21]. The optimization circuit reads in the response of the target circuit, compares it with the expected circuit, and selects the optimal tuning knob values, such that the effect of process variations is minimized.

3 Locking approach for AMS circuit

In this section, we first describe a BPF circuit, which we will use as a motivational example to explain our idea. We then describe our locking architecture, and the methodology to describe how it is used to select an optimal set of tuning knobs for the maximum impact. Finally, we are explaining how the proposed mechanism is applicable to other analog circuits, such as LNA and LDO.

3.1 Motivational example: Band-pass filter

Consider the Tow-Thomas filter of Fig. 2 with a transfer function defined by Eqn 1.

$$H_{BP}(s) = \frac{s/(R_1C)}{s^2 + s/(R_1C) + 1/(R_2^2C^2)} \quad (1)$$

Assuming ideal amplifiers (amplifiers with large enough gain and bandwidth), $R_1 = R_3$, and $R_2 = R_4$ the characteristics of the filter like center frequency $\omega_o = 1/(R_2C)$ and quality factor $Q = R_1/R_2$ are defined by the passive components, i.e., resistors and capacitors. In order to provide tuning, the passive components are actually implemented by arrays of resistors and capacitors. Such tuning helps to compensate for any changes in resistor and capacitor values due to process variations. The parameters ω_o and Q are estimated on-chip by measuring the amplitude at four frequency points determined by the central frequency and the filter's bandwidth [21]. The cost function of the optimizer quantifies the error between the amplitudes at f_1 vs. f_4 and f_2 vs. f_3.

3.2 Locking architecture

The AMS design in Fig. 3 consists of the BPF circuit to be protected along with the analog to digital converter (ADC) and the logic-locked optimizer. The voltage input and control bits of the two tuning knobs from the optimizer are the inputs to the BPF. Each

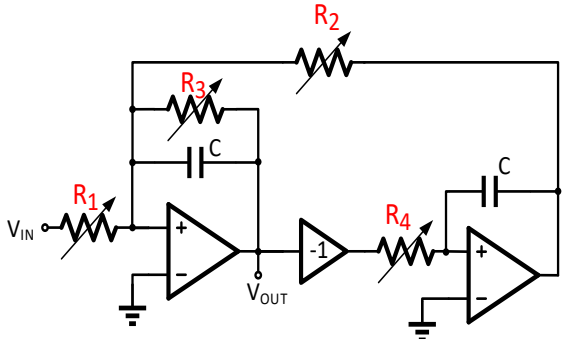

Figure 2: Tow-Thomas BPF circuit. The resistors R_1, R_2, R_3, and R_4 are the tuning knobs.

tuning knob setting corresponds to a unique value of the resistor in the BPF circuit which in turn has an impact on its frequency response. During the start-up, the tuning knobs are in their default settings. Once the input voltage is applied to the BPF, the output is converted to digital by ADC and sent to the logic-locked optimizer. The secret key required for the proper operation of this optimizer is loaded from a tamper-proof memory. The optimizer calculates the cost difference in the measured and the desired output response of the BPF. If the magnitude of this difference is high, it indicates that the BPF response is far away from the desired response and if low, indicates it is more close to the desired response.

As the tuning knob settings solely depend on the optimizer, logic locking this unit ensures that it chooses the tuning knob which produces undesired output response from the analog circuit when an incorrect key is given. To be more specific, the MSB of the cost difference is protected. When an incorrect key is given, the MSB of this cost flips. Hence the optimizer sees the cost with a low magnitude as high and vice-versa. Therefore, it tunes the analog circuit incorrectly. On the other hand, when a right key is given, it ensures normal circuit operation.

This simple architecture suffers from two challenges:

Issue 1: Not all resistors and capacitors in the BPF need to be tuned. This is because, making every component tunable increases the overhead of those components, and also the optimizer circuity now has to optimize more variables, which in turn increases its overhead. Thus, one needs to judiciously select the variables to tune.

Issue 2: The logic locking techniques can protect only a small number of input patterns. For instance, *HD-0* can protect only one input pattern with a security level of k, and *HD-h* can protect $2^{n-k} \cdot \binom{k}{h}$ patterns with a security level of $k - log_2\binom{k}{h}$.

Hence, one has to judiciously select the input patterns of the AMS circuit (i.e., responses of the AMS circuit) need to be protected.

3.3 Sensitivity analysis to solve Issue 1

In circuit analysis, sensitivity is a measure of the variation in a performance metric caused by a change in a certain circuit parameter [3]. The normalized sensitivity of f_i w.r.t. the parameter x_j is represented by the Eqn. 2. Since it allows to compare the effect of each parameter in a circuit specification, it is a useful tool for designing analog circuits.

$$S_{x_j}^{f_i} = \frac{x_j}{f_i}\frac{\partial f_i}{\partial x_j} \tag{2}$$

In order to minimize the error in the performance metrics due to PVT variations, circuit parameters have to be tuned. By using the sensitivity analysis, the designer can choose the tuning knobs and design their range in a smart way. This task is performed in four steps. First, the overall range in the circuit performance metrics due to variations and performance flexibility is determined. Secondly, the sensitivity of the performance metrics w.r.t different circuit parameters (possible tuning knobs) is calculated and ranked. Third, the tuning knobs are selected considering their sensitivity and the implementation complexity and overhead. Finally, the tuning range is designed. For the BPF, the center frequency and the quality factor are the performance metrics on which this analysis is performed. The selected tuning knobs are the resistors R_1 and R_2. The same procedure can be applied to different circuit topologies in order to make them flexible and robust against process variations.

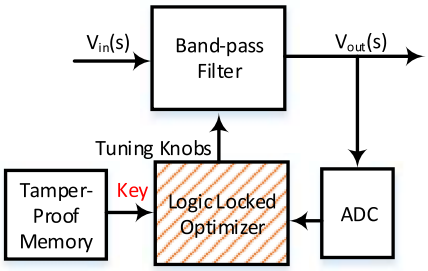

Figure 3: Logic locking of the BPF circuit.

3.4 Choosing input patterns to solve Issue 2

In case of *HD-0*, since only one input pattern can be protected, it is obvious to select the input pattern of the optimizer that results in the minimum cost function. For instance, in case of BPF, we need to protect the input pattern corresponding to resistor settings $R_1 = 27.68K\Omega$ and $R_2 = 10.38K\Omega$, as this makes the optimizer to yield the minimum cost function value. In other words, this is the input pattern, for which the error between the expected response and the actual response of the BPF is minimum, as shown in Fig. 4.

In case of *HD-h*, a designer can increase the number of input patterns protected by increasing value of h. However, this decreases the security level of an n-bit design by $2^{n-k} \cdot \binom{k}{h}$. Hence, one can increase the value of h only to an extent. In case of BPF, the optimizer has 220-bit input, for which the maximum value of h can be 37, the maximum number of input patterns protected can be 1.37×10^{42}.[1] Here, we select those input patterns such that they are at a Hamming distance h away from the one that produces the minimum cost function.

3.5 Extending to other AMS circuits

The locking architecture has been tested in a BPF, however it can be used to secure different analog circuits. Two of them are:

3.5.1 LNA A common gate LNA was tested as a study case [11]. The specifications to optimize are the gain (S_{21}) and the input matching (S_{11}) for the given resonance frequency. Based on sensitivity

[1]This is assuming a security level of 80, which is the standard security practice.

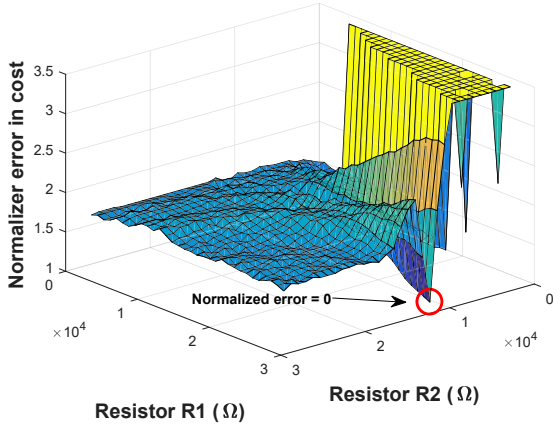

Figure 4: Normalized error on the output of BPF for different tuning knobs. The normalized error at $(27.68K\Omega, 10.38K\Omega) = 0$. The data is collected from a IBM-180nm process BPF chip described in Section 4.

Table 1: Effect of *HD-0* and *HD-h* logic locking techniques on the optimizer circuits of BPF, LNA, and LDO. In case of BPF, the data is collected from the IBM-180nm process BPF chip described in Section 4. The correct values of the tuning knobs for BPF are $(27.68K\Omega, 10.38K\Omega)$. We used simulation results for LNA and LDO. % error listed is the minimum error on applying any incorrect key.

Analog Circuit	# of inputs	Key size	Security level (s)	# of patterns protected	% error (min.)	Key size	Hamming distance (h)	Security level (s)	# of patterns protected	% error (min.)
Band-pass filter	220	220	220	1	8.11	220	1	212	220	8.11
	220	112	112	3.25×10^{32}	44.59	220	20	126	1.19×10^{28}	8.11
	220	87	87	1.09×10^{40}	72.97	220	37	80	1.37×10^{42}	8.11
Low noise amplifier	154	154	154	1	0	154	1	146	154	0
	154	84	84	1.18×10^{21}	3100	154	9	107	1.06×10^{14}	0
	154	81	81	9.44×10^{21}	3100	154	17	80	1.73×10^{22}	0
Low-dropout regulator	234	234	234	1	0.7	234	1	226	234	0.7
	234	135	135	6.34×10^{29}	12.59	234	20	138	4.32×10^{28}	0.7
	234	109	109	4.25×10^{37}	39.58	234	41	81	9.89×10^{45}	0.7

analylsis, the tuning knobs are determined to be the biasing current and the capacitance of the load tank. These two metrics are estimated by applying two frequency tones at $f_R \pm \Delta_f$ and connecting the proper matching at the input and output. Then, the signal's amplitude is measured at the input and output of the LNA. The cost function measure the error of the gain at two frequencies and the error between the amplitude of the input applied and the one seen at the LNA's input at the two tones.

3.5.2 LDO voltage regulator A capless LDO with PMOS pass transistor and a single stage error amplifier is tested [17]. The performance metrics to optimize are the power supply rejection (PSR) and the phase margin. The selected tuning knobs are the biasing current of the error amplifier and the compensation capacitor. The PSR is measured directly by applying a sine wave at the input and measuring an amplified version of the voltage at the output. On the other hand, the phase margin is measured indirectly as the peaking in the loop gain.

4 Results

4.1 Experimental setup

For our experiments, we demonstrate the logic-locking techniques on three different AMS circuits: BPF, LNA, and LDO. The specifications for each of these circuits are as follows. The bandpass filter has a center frequency $f_c = 74MHz$ and $BW = 13MHz$. The input to the optimizer has 220 bits, which include the BPF frequency response data from ADC and the weights used in the cost calculation. The specifications of the LNA circuit are $S_{21} > 20dB$ and $S_{11} < -20dB$ at a resonance frequency $f_R = 6GHz$, with input size to the optimizer equal to 154 bits. Similarly, the LDO's specifications are $PSR \leq -50dB$ and a phase margin larger than 45° with optimizer input size equal to 234 bits. The optimizer implements a simulated annealing algorithm.

The experiments are executed on 40, 10-core Intel Xeon processors running at 2.8GHz with 256 GB of RAM. The designs are synthesized using Synopsys Design Compiler tool using Nangate 45nm open cell library [5].

Measurement setup: The data of the BPF optimization circuit was collected from the measurement setup. Fig. 5 shows the printed circuit board (PCB) with the BPF fabricated using IBM-180nm process. The optimizer is implemented on an FPGA and a dual voltage source was used as supply. As the impact of process variation is more prominent in smaller technology nodes, our locking approach will be more effective as the technology scales.

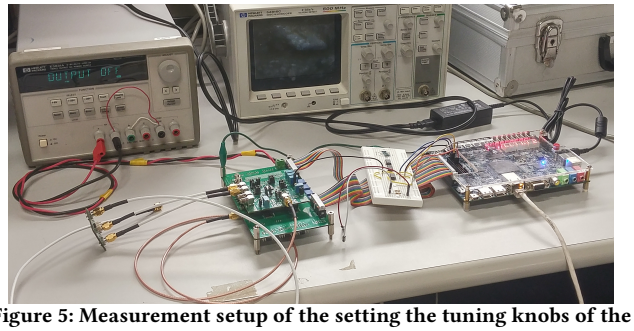

Figure 5: Measurement setup of the setting the tuning knobs of the BPF circuit.

4.2 Effect of tuning knobs on BPF's output

In order for the locking technique on the BPF circuit to be effective, any deviation in the tuning knob values from its ideal set of values should degrade the BPF's response. This effect can be quantified by normalized error value. Figure 4 shows the normalized error value for different tuning knob values. As one can see, when the (R1,R2) values are (27.68KΩ, 10.38KΩ), the normalized error value is zero, and for all the other cases, there is a non-zero error. Thus, only on setting the tuning knobs to the correct values, the desired response is obtained. Any deviation from these correct values indicates an incorrect response from the BPF circuit.

4.3 Effect of logic locking on tuning knob

As mentioned earlier, only on applying the correct key, the locked optimizer circuit sets the tuning knobs to the correct value. However, both *HD-0* and *HD-h* techniques can protect only a handful input patterns. Hence, one has to select the input patterns that result in the optimal tuning knob values and protect them, while ensuring the security guarantees at the same time.

Table 1 lists the effect of *HD-0* and *HD-h* logic locking techniques on the optimizer circuits of BPF, LNA, and LDO. In case of *HD-0*, when the key size equals the input size of the optimizer circuit, $k = n = 220$, the Hamming distance $h = 0$, and only one input pattern can be protected. Based on the normalized error in Fig. 4, we choose to protect the pattern that results in the minimum error. Hence, the input pattern resulting in the ideal tuning knob values, i.e., $(27.68K\Omega, 10.38K\Omega)$ is protected; in this case, the normalized error is 0%. For any incorrect key, the optimizer sets the tuning knob that results in a normalized error value of at least 8.11%. Though the security level (s) achieved by this approach is 220, the normalized error value is only 8.11%.

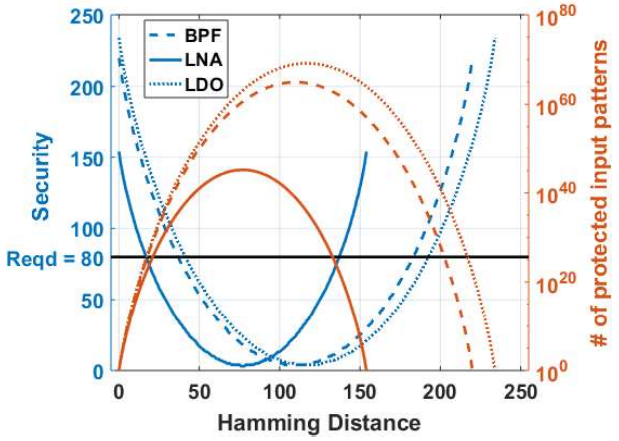

Figure 6: For *HD-h* technique, the effect of Hamming distance vs. SAT attack resiliency and the number of input patterns protected for BPF, LNA, and LDO. The right-hand side y-axis is in log scale.

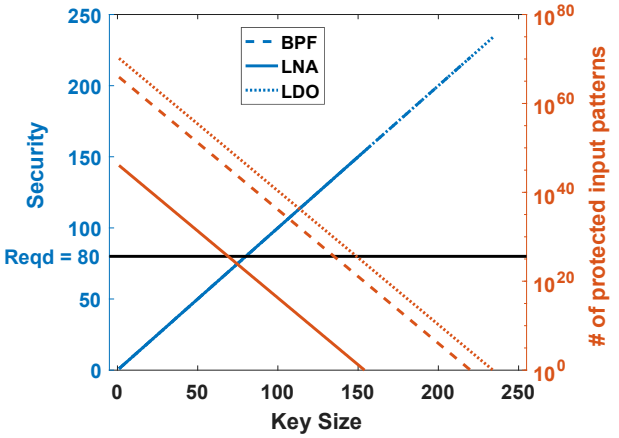

Figure 7: Key size vs. SAT attack resiliency and the number of input patterns protected for BPF, LNA, and LDO. The right-hand side y-axis is in log scale. The Hamming distance $h = 0$. The security level achieved by BPF, LNA, and LDO are the same and hence are superimposed.

One approach to increase the error value is to protect more number of inputs patterns. This can be achieved by reducing the key size. For instance, for *HD-0* and a key size of $k = 112$, the number of input patterns protected is 3.25×10^{32}, increasing the normalized error to 44.59%. Similarly, by choosing a key size of $k = 87$, a normalized error value is increased to 72.97%. However, one cannot reduce the key size below 80 bits, because this reduces the s and hence the search space to less than 2^{80}, making it vulnerable to SAT and brute-force attacks. Another approach to increase the number of protected input patterns and hence the normalized error value is to use *HD-h*, whose results in Table 1.

In case of LNA, *HD-0* and *HD-h* achieve the normalized error rate of 3100% and 0%, respectively. For LDO, *HD-0* and *HD-h* obtain the normalized error rate of 39.58% and 0.7%, respectively. As one can see, for the same key size, *HD-h* protects more input patterns compared *HD-0*. For instance, in case of BPF, for a key size of 220, *HD-0* protects only one input pattern, whereas *HD-h*, for $h = 37$, protects 1.37×10^{42}. However, the normalized error rate is still the same (i.e., 8.11%) or even lesser (i.e., for LNA it is 0%). This is because *HD-h* requires all the protected input patterns to have the same Hamming distance from the key with key size equal to input size. The probability of all the patterns protected having the same h is very small. This indicates that *HD-0* results in a higher error than *HD-h*.

4.4 Security analysis

This work protects the desired output response of AMS circuits from the attackers rather than the circuit topology itself. This is done by controlling the values of the analog circuit parameters, (i.e, R and C) by the logic locked optimizer. Hence the security of the complete AMS circuit is the security offered by the logic locked optimizer. The following section shows the resiliency offered by the locked optimizer.

Resiliency against SAT. The resiliency against SAT attack offered by *HD-0* and *HD-h* are k and $k - log_2\binom{k}{h}$, respectively [25]. From Fig. 6, we can infer that security level s achieved for the BPF is the maximum when Hamming distance $h = 0$ or $h = 220$ and the minimum when $h = 110$. In order to ensure that the locked circuit is SAT-attack resilient, we need to choose h and k such that the security level is greater than 80. Hence, the allowable h values can be $0 \leq h \leq 37$ or $183 \leq h \leq 220$, and the corresponding number of input patterns which can be protected are $1 <$ # of patterns protected $< 1.37 \times 10^{42}$. Similarly, for LNA, the allowable value of h is $0 \leq h \leq 17$ or $137 \leq h \leq 154$ and the number of input patterns which are protected ranges $(1, 1.73 \times 10^{22})$. For the LDO, $0 \leq h \leq 41$ or $193 \leq h \leq 234$ and the input patterns protected are in the range $(1, 9.89 \times 10^{45})$.

Also from Fig. 7, the security increases with the increase in key size whereas the number of input patterns protected reduce with the increase in key size. To ensure resiliency against the SAT-attack, the key size should be $k > 80$. Hence the number of input patterns which can be protected ranges $(1, 1.39 \times 10^{42})$ for BPF. Likewise, the number of input patterns protected for LNA ranges $(1, 1.89 \times 10^{22})$ and that of LDO is $(1, 2.28 \times 10^{46})$.

To analyze the time taken for the SAT attack, the logic-locked optimizer of the BPF circuit is subject to this attack. The time required for the attack, as shown in Fig. 8, increases exponentially with the input size. For the input size of 14, the attack takes close

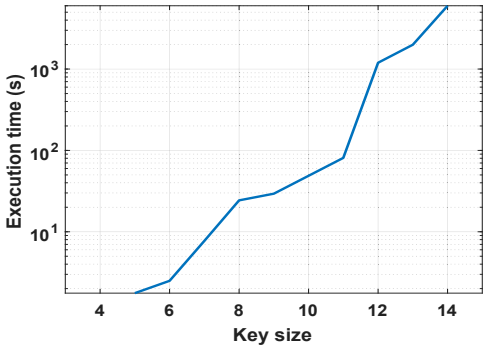

Figure 8: Execution time of the SAT attack for BPF. The time required for the attack to find the key increases exponentially with respect to key size. Note that y-axis is in log scale.

to 1.5 hours to identify the key. This indicates that our technique is secure against SAT attack. Similarly, it is also secure against AppSAT [14], as we protect only a linear number of input patterns.

Resiliency against removal attack [24]. An attacker cannot remove the locked optimizer circuit and make the analog circuit functional because the tuning knobs will not be set to optimal values due to process variations, thus preventing removal attacks. If he removes the locked optimizer unit, the circuit parameters will be fixed to the default value. The probability of this value being the desired value to address process variations is negligible. An attacker cannot set the tuning knob value to its optimal value through a focused-ion-beam (FIB) because even identifying the value of one chip cannot be used to set the value for another chip, as the values will be different because of process variations. In other words, the amount of compensation varies one chip to another chip.

Resiliency against bypass attacks [23]. Bypass attacks use two keys to maximize the number of correct patterns. Since we are using SFLL, our technique is inherently secure against bypass attacks [23].

4.5 Effect of incorrect keys

The response of the circuits for a correct and an incorrect key are compared. Fig 9(a) shows the difference in the frequency response of the BPF. In this case, the correct key allows the optimizer, tune the circuit to the target ω_o and BW, while an incorrect key forces the optimizer to tune to a lower frequency and also reduces the Q and gain values. Fig. 9(b) compares the difference in the S-parameters of the LNA targeting $f_R = 6GHz$. One can observe an error of $1GHz$ in f_R and an error on S_{11} and S_{21} of at least 15 dB. Finally, the deviation on the LDO performance for the two cases was evaluated. Fig. 9(c) shows a degradation close to 10dB in the PSR. Fig. 9(d) shows a large peaking on the loop gain for the wrong key, which indicates low phase margin and potential instability.

4.6 Discussion

Why not protect all the digital components in AMS circuit? A simple solution is to protect all the digital components of the AMS circuit. However, this seemingly straightforward approach is not simple and may not meet the desiderata for analog circuits, for reasons below.

The desiderata for protecting AMS circuit via logic locking of digital components:

- An attacker should not be able to identify the locked digital part, remove it, and make the resultant analog circuit functional[2].
- Logic locking the entire digital circuit may not necessarily yield incorrect responses from the analog part. Hence, the digital circuit needs to be locked such that analog component becomes non-functional when an incorrect key is applied.
- State-of-the-art logic locking techniques can protect only a linear number of input patterns in key size [25]. Hence, one needs to select which input patterns to protect, such that incorrect keys will have the highest impact on the functionality of the analog circuit.
- Locking the entire circuit incurs high area, power, and delay overhead. Hence, one has to be judicious in selecting which components to protect.

[2]Here, we consider an analog design as functional when it produces the expected response.

Area, power, and delay overheads. In this implementation, the power overhead is not a concern since the optimization and security platform is consuming power only at the start time for a short period. Once the optimization finds a solution and sets the controlling bits of the tuning knobs, the digital core is turned off.

There is a delay between the time at which the circuit is turned on and the time at which it actually starts the normal operation. This delay involves the optimization time, but this does not impact the response time of the circuit.

Area overhead of *HD-0* for BPF, LNA, and LDO is 8.79%, 2.61%, and 3.08%, respectively. Similarly, for *HD-h*, the overhead is 8.78%, 5.84%, and 4.91%, respectively, for the h values listed in Table 1.

Effect of aging, temperature, and environmental noise. The on-chip optimizer circuit can measure the performance of the AMS circuit: the physical parameters of the chip, including their degradation due to aging, and the conditions of operation such as the temperature and the noise on the supply. Thus, the optimizer circuit can retune its tuning knob values to obtain the desired response—but only when the correct key is in place. Thus, our technique can ensure the effect of locking, even in the presence of aging and environmental effects.

5 Conclusion

In this paper, we propose the first technique to thwart the overproduction of AMS circuits, by securely locking the digital part, which is controlling the tuning knobs judiciously. Our analysis indicates that by properly selecting two tuning knobs we can secure several performance metrics of different analog circuits—a BPF, an LNA, and an LDO. On applying an incorrect key, our approach achieves at least 8% error and at most 73% error in the circuit's response. For LNA, *HD-0* achieves a better error rate than *HD-h*. Our technique is agnostic to logic locking techniques: we have used SFLL [25], as it can prevent SAT [16], AppSAT [14], removal [24], sensitization [9], and bypass attacks [23]. Our approach is provably-secure, as it leverages the properties of SFLL. More importantly, it is well integrated with the analog component, without sacrificing the security properties of SFLL. However, one can always use other logic locking techniques as well.

Our future work entails: (i) Exploring the effect of other logic locking techniques; (ii) Embedding secret keys as part of analog designs, not just digital; and (iii) Exploring techniques to prevent piracy and not just overproduction.

6 Acknowledgement

This work is partially supported by National Science Foundation CNS-1618824, CNS-1828840, STARSS-1618797 and SATC CAREER-1822848, and Intel. The authors would also like to thank J. Wang, A. Sengupta, and C. Shi for their help.

References

[1] A. Baumgarten, A. Tyagi, and J. Zambreno. 2010. Preventing IC Piracy Using Reconfigurable Logic Barriers. *IEEE Design & Test of Computers* 27, 1 (2010), 66–75. https://doi.org/10.1109/MDT.2010.24

[2] Yu Bi, Jiann Yuan, and Yier Jin. 2015. Beyond the Interconnections: Split Manufacturing in RF Designs. *MDPI Electronics* 4, 3 (2015), 541–564. https://doi.org/10.3390/electronics4030541

[3] I. Guerra-Gómez, E. Tlelo-Cuautle, and Luis G. De La Fraga. 2013. Richardson Extrapolation-based Sensitivity Analysis in the Multi-objective Optimization of Analog Circuits. *Applied Mathematics and Computation* 222 (2013), 167–176. https://doi.org/10.1016/j.amc.2013.07.059

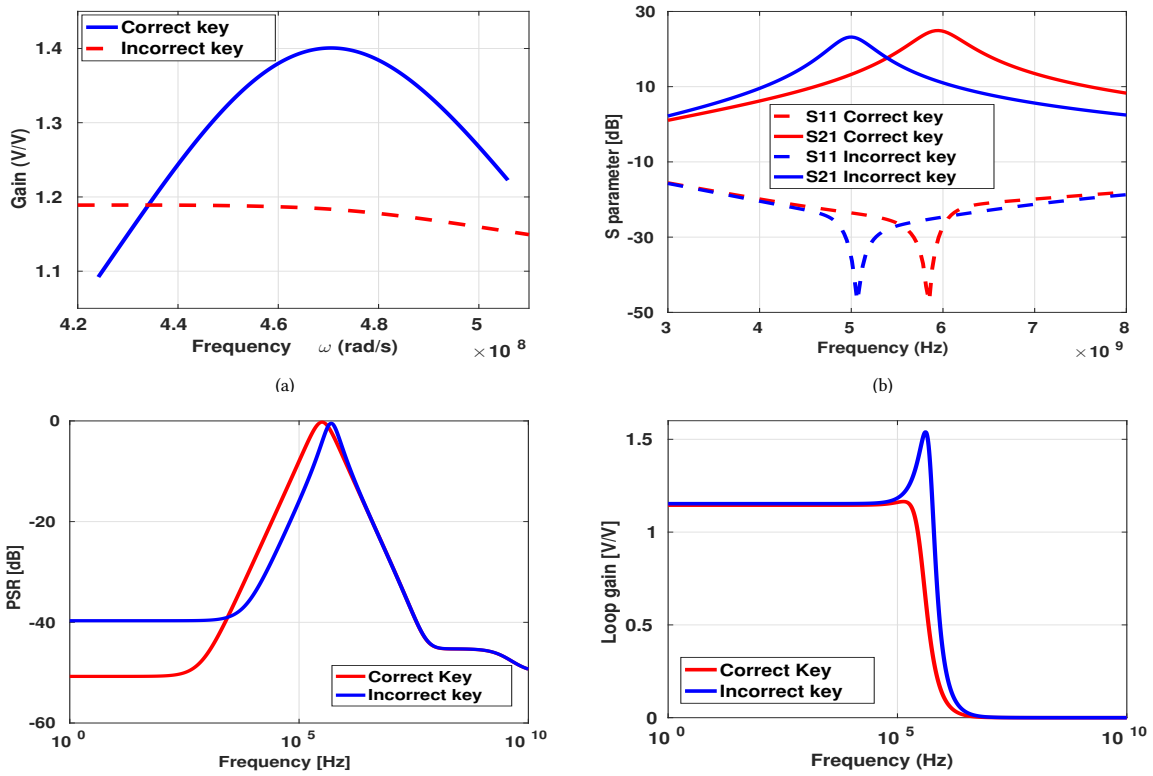

Figure 9: Behavior of the analog circuits for correct and incorrect keys on using *HD-0*. The key size used for BPF, LNA, and LDO are 87, 81, and 109, respectively. (a) Frequency response of BPF, (b) S-parameters of LNA, (c) Power supply rejection (PSR) of LDO, and (d) Loop gain of LDO.

[4] D. H. K. Hoe, J. Rajendran, and R. Karri. 2014. Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors. *IEEE Computer Society Annual Symposium on VLSI* (2014), 516–521. https://doi.org/10.1109/ISVLSI.2014.50

[5] Nangate Inc. 2011. NanGate FreePDK45 Open Cell Library. http://www.nangate.com/?page_id=2325. Last accessed the website on 06/30/18.

[6] Maxim Integrated. 2010. DeepCover Security Manager for Low-Voltage Operation with 1KB Secure Memory and Programmable Tamper Hierarchy. https://www.maximintegrated.com/en/products/power/supervisors-voltage-monitors-sequencers/DS3660.html/tb_tab0.

[7] Trent McConaghy, Kristopher Breen, Jeffrey Dyck, and Amit Gupta. 2013. *Variation-Aware Design of Custom Integrated Circuits: A Hands-on Field Guide.* Springer, New York, NY, USA.

[8] T. S. Perry. 2017. Why Hardware Engineers Have to Think Like Cybercriminals, and Why Engineers Are Easy to Fool. http://spectrum.ieee.org/view-from-the-valley/computing/embedded-systems/why-hardware-engineers-have-to-think-like-cybercriminals-and-why-engineers-are-easy-to-fool

[9] Jeyavijayan Rajendran, Youngok Pino, Ozgur Sinanoglu, and Ramesh Karri. 2012. Security analysis of logic obfuscation. *IEEE/ACM Design Automation Conference* (2012), 83–89. https://doi.org/10.1145/2228360.2228377

[10] V. V. Rao and I. Savidis. 2017. Parameter Biasing Obfuscation for Analog IP Protection. *IEEE Latin American Test Symposium* (2017), 1–6. https://doi.org/10.1109/LATW.2017.7906739

[11] B. Razavi. 2011. *RF Microelectronics.* Pearson Education.

[12] M. Rostami, F. Koushanfar, and R. Karri. 2014. A Primer on Hardware Security: Models, Methods, and Metrics. *Proceedings of the IEEE* 102, 8 (2014), 1283–1295. https://doi.org/10.1109/JPROC.2014.2335155

[13] J. A. Roy, F. Koushanfar, and I. L. Markov. 2010. Ending Piracy of Integrated Circuits. *Computer* 43, 10 (Oct 2010), 30–38. https://doi.org/10.1109/MC.2010.284

[14] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, and Y. Jin. 2017. AppSAT: Approximately deobfuscating integrated circuits. *2017 IEEE International Symposium on Hardware Oriented Security and Trust* (2017), 95–100. https://doi.org/10.1109/HST.2017.7951805

[15] Solid State Technology. 2012. Top 5 counterfeited semiconductors: analog ICs top the list–solid state technology. http://electroiq.com/blog/2012/04/top-5-counterfeited-semiconductors-analog-ics-top-the-list/.

[16] P. Subramanyan, S. Ray, and S. Malik. 2015. Evaluating the security of logic encryption algorithms. *IEEE International Symposium on Hardware Oriented Security and Trust* (2015), 137–143. https://doi.org/10.1109/HST.2015.7140252

[17] J. Torres, M. El-Nozahi, A. Amer, S. Gopalraju, R. Abdullah, K. Entesari, and E. Sanchez-Sinencio. 2014. Low Drop-Out Voltage Regulators: Capacitor-less Architecture Comparison. *IEEE Circuits and Systems Magazine* 14, 2 (2014), 6–26. https://doi.org/10.1109/MCAS.2014.2314263

[18] Chris Toumazou, George Moschytz, and Barrie Gilbert. 2002. *Trade-offs in analog circuit design.* Kluwer Academic Publishers.

[19] P. Tuyls, G. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters. 2006. Read-Proof Hardware from Protective Coatings. *International Conference on Cryptographic Hardware and Embedded Systems* (2006), 369–383.

[20] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu. 2017. Thwarting analog IC piracy via combinational locking. *IEEE International Test Conference* (2017), 1–10. https://doi.org/10.1109/TEST.2017.8242064

[21] J. Wang, C. Shi, E. Sanchez-Sinencio, and J. Hu. 2015. Built-In Self Optimization for Variation Resilience of Analog Filters. *IEEE Computer Society Annual Symposium on VLSI* (2015), 656–661. https://doi.org/10.1109/ISVLSI.2015.79

[22] Y. Xie and A. Srivastava. 2016. Mitigating SAT Attack on Logic Locking. *International Conference on Cryptographic Hardware and Embedded Systems* (2016), 127–146.

[23] Xiaolin Xu, Bicky Shakya, Mark M. Tehranipoor, and Domenic Forte. 2017. Novel Bypass Attack and BDD-based Tradeoff Analysis Against All Known Logic Locking Attacks. *CHES* (2017). https://doi.org/10.1007/978-3-319-66787-4_10

[24] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran. 2017. Security analysis of Anti-SAT. *22nd Asia and South Pacific Design Automation Conference* (2017), 342–347. https://doi.org/10.1109/ASPDAC.2017.7858346

[25] Muhammad Yasin, Abhrajit Sengupta, Mohammed Thari Nabeel, Mohammed Ashraf, Jeyavijayan (JV) Rajendran, and Ozgur Sinanoglu. 2017. Provably-Secure Logic Locking: From Theory To Practice. *Proceedings of ACM SIGSAC Conference on Computer and Communications Security* (2017), 1601–1618. https://doi.org/10.1145/3133956.3133985