Securing Analog Mixed-Signal Integrated Circuits Through Shared Dependencies

Kyle Juretus*
Drexel University
Philadelphia, Pennsylvania 19104
kjj39@drexel.edu

Vaibhav Venugopal Rao*
Drexel University
Philadelphia, Pennsylvania 19104
vv85@drexel.edu

Ioannis Savidis
Drexel University
Philadelphia, Pennsylvania 19104
isavidis@coe.drexel.edu

ABSTRACT

The transition to a horizontal integrated circuit (IC) design flow has raised concerns regarding the security and protection of IC intellectual property (IP). Obfuscation of an IC has been explored as a potential methodology to protect IP in both the digital and analog domains in isolation. However, novel methods are required for analog mixed-signal circuits that both enhance the current disjoint implementations of analog and digital security measures and prevent an independent adversarial attack of each domain. This paper demonstrates the vulnerabilities of implementing disjointed obfuscation techniques to protect analog mixed-signal ICs. In addition, a novel methodology is developed to generate functional and behavioral dependencies between the analog and digital domains that results in an increase in the adversarial key search space. The dependencies between the analog and digital keys result in a 3x increase in the number of iterations required to complete the SAT attack. An analysis of best practices is also provided to aid in the implementation of security measures for analog mixed-signal circuits.

KEYWORDS

logic locking, parameter locking, SAT attack, hardware security

ACM Reference Format:
Kyle Juretus, Vaibhav Venugopal Rao, and Ioannis Savidis. 2019. Securing Analog Mixed-Signal Integrated Circuits Through Shared Dependencies. In *Great Lakes Symposium on VLSI 2019 (GLSVLSI '19), May 9–11, 2019, Tysons Corner, VA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3299874.3319497

1 INTRODUCTION

Malicious modifications to integrated circuits (ICs) represent a serious threat to the security of the entire computing stack, with back doors [1] and a variety of counterfeit ICs [2, 3] having already been discovered within military ICs. The security threats at the hardware level are expected to increase as the IC manufacturing flow transitions to a horizontal model, where manufacturing, testing, and intellectual property (IP) are procured from third-parties [3]. Untrusted third-parties within the IC design flow possess the ability to steal IP, counterfeit and overproduce ICs, and insert harmful circuit modifications (hardware Trojans).

According to a report by Information Handling Services (IHS) Markit [4], the top five most counterfeit types of semiconductors include analog ICs, microprocessors, memory, programmable logic ICs, and discrete transistors, which represents an annual potential risk of approximately $169 billion to the semiconductor supply chain [4]. To address the pertinent security issues of IP theft, overproduction, reverse engineering, counterfeiting, Trojan insertion, and data hacking effectively, hardware level design-for-trust techniques including logic locking [5–7], watermarking [8, 9], camouflaging [10], and IC metering [11] have been proposed. The majority of hardware security measures are only applicable to digital circuits and are not suitable for implementation on analog circuits.

The security of analog mixed-signal (AMS) circuits, however, is of importance as 25% of the reported counterfeit incidences [4] occur in AMS systems. In addition, there is a large increase in demand for analog mixed-signal circuits with varied capabilities due to a growing demand for Internet of Things (IoT) devices, which are used in a wide array of applications from household products to defense systems. According to an IHS report, the number of IoT devices is estimated to increase by around 200% from 2019 to 2025 [12]. As more and more IoT devices are produced, securing the circuits against hardware security threats including counterfeiting, overproduction, reverse engineering, and Trojan insertion becomes challenging. As AMS systems are vulnerable to a wide range of threat vectors, the unsecured analog circuit blocks also present an exploitable point of entry to the IC even when the digital IP is protected.

To address the growing need of protecting AMS IP, this paper proposes a novel methodology to concurrently secure both analog and digital circuit blocks. The analog block is protected with a parameter based obfuscation technique [13] that masks the dimensions of the transistors used to implement vital components of the analog circuit. The analog circuit only operates as intended when the correct key is applied. The digital portion of the AMS circuit is protected with two different logic locking strategies; the XOR methodology [5] and the modified logic cone methodology [14]. The correct functionality of the digital block is also dependent on the application of the correct key to the circuit.

An analysis of the security of independently locked analog and digital circuit blocks is provided. An attack that isolates the analog and digital circuit blocks is described, limiting the effective key space of the secured circuit. The analog and digital blocks are modified to include correlated key dependencies within the circuit, which results in an increase in the level of difficulty to attack the IC.

*These authors contributed equally to this work

GLSVLSI '19, May 9–11, 2019, Tysons Corner, VA, USA

ACM ISBN 978-1-4503-6252-8/19/05…$15.00
https://doi.org/10.1145/3299874.3319497

Both the analog and digital circuits are attacked with a satisfiability modulo theory (SMT) based technique that explores the logical and functional search space generated by a 16-bit key, where the attack is characterized by the number of iterations required to determine the correct key. The primary contributions of this paper include:

(1) protection of analog mixed-signal circuits by obfuscating both the analog and digital sub-components,
(2) an analysis of the security of the analog mixed-signal circuit using a SMT based search space exploration technique, and
(3) the development of a novel methodology to generate functional and behavioral dependencies between the analog and digital domains that results in an increase in the adversarial key search space.

The paper is organized as follows. Recent techniques to protect digital, analog, and AMS circuits are described in Section 2. The assumed threat model is provided in Section 3. An overview of the proposed obfuscation technique and the implementation of the technique on an AMS circuit is described in Section 4.1 and 4.2, respectively. The limitation of independently securing analog and digital blocks is analyzed in Section 4.3. A methodology to generate dependencies between the analog and digital circuit blocks is described in Section 5. Best practices to secure AMS circuits are described in Section 6. Some concluding remarks are provided in Section 7.

2 PRIOR RESEARCH ON CIRCUIT OBFUSCATION

An overview of prior research to secure digital, analog, and AMS circuits is provided in this section.

2.1 Digital Logic Locking

Extensive research on logic locking techniques that protect digital IP have previously been reported. There are two distinct categories of digital logic locking techniques: 1) methods that obfuscate within the logic cone, and 2) the addition of circuitry that produces errors in circuit functionality when an incorrect key is applied. Techniques that insert XOR/XNOR [5], LUT [6], and MUX [7] based secure gates within the original logic cone have been developed. Optimization of circuit locking techniques to lower the overhead in power, area, and performance [15, 16] and selection algorithms to determine the optimal insertion point of the secure gates in the circuit [7, 17–19] have also been reported.

The SAT attack proposed in [20] resulted in the development of techniques that add additional circuitry to increase the total number of distinguishing input patterns (DIPs) needed to successfully execute the SAT attack [14, 21–24]. However, while the methodologies provide a provable means to quantify the number of iterations required to execute the SAT attack, some of the methods are vulnerable to the removal of the added circuitry [25]. To prevent removal attacks, more recent techniques, such as described in [14] and [24], alter the original logical functionality of the IC and implement added circuitry to rectify the altered minterms when the correct key is applied.

2.2 Analog Logic Locking

A key-based locking/unlocking mechanism for a sense amplifier circuit is proposed in [26]. A memristor-based voltage divider is implemented to provide a variable voltage bias to the body of the transistors of the sense amplifier. A memristor crossbar structure allows for the programming of the voltage divider, which results in the correct circuit functionality only when the correct 16-bit key is applied. The practical application of the method is limited as memristors are not readily available and the fabrication of the memristors is incompatible with standard CMOS processes.

The current mirror based combinational locking technique proposed in [27] utilizes transistors of different sizes to mask the current gains of the analog circuit. Based on the applied key sequence, a range of current values are set. A satisfiability modulo theory (SMT) based algorithm is used to generate a unique key. The primary disadvantage of current mirror based combinational locking is that the technique is limited to masking the biasing currents of an analog circuit.

Key based performance locking of analog circuits is proposed in [13, 27, 28], where locking circuitry is inserted into an analog IC to mask biasing conditions, gains, operating frequencies, and performance parameters. In the parameter obfuscation technique proposed in [13] and [28], the sizes of the transistors used to set the optimal biasing conditions are masked using parallel (vector) and mesh-based transistor arrays. Based on the applied key, a subset of the transistors in the vector or mesh are activated to produce an overall effective transistor width over length ratio $\left(\frac{W}{L}\right)_{eff}$. Proper analog circuit functionality is only achieved when the correct key is applied. The SMT based search space exploration methodology proposed in [29] is applied to ensure that only a single correct key exists that sets the optimal circuit performances and that incorrect keys result in significant degradation in the performance of the analog circuit blocks (i.e. eliminate keys that set "good enough" performance values).

2.3 AMS Logic Locking

The logic locking methodologies described in [30] and [31] obfuscate the digital part of the mixed-signal IC. Specifically, the stripped-functionality logic locking (SFLL) [14] technique is implemented on the digital portion of the circuit to lock the entire mixed-signal IC. Digital circuitry responsible for the post-silicon tuning of the analog circuits is obfuscated using the SFLL logic locking technique in [31]. The primary disadvantage of only obfuscating the digital portion of an AMS IC is that no protection is offered to the purely analog blocks. In addition, all prior work to secure AMS circuits applied techniques that independently protect the analog and/or digital blocks. An analysis of applying disjoint security measures to the analog and digital circuit blocks of an AMS IC is, therefore, provided in Section 4.3. In addition, a methodology to generate a functional and behavioral dependency between the analog and digital circuit domains is developed in Section 5 that increases the security and effective key space of the IC.

3 THREAT MODEL

The threat model for this work assumes that an adversary possesses the tools and knowledge necessary to reverse engineer the IC and produce an extracted locked netlist representation of the circuit. To obtain the logically functional representation of the circuit, an adversary must determine the correct keys for the obfuscated portions of the IC. In addition, an adversary is assumed to possess

an activated IC, which is used to obtain input-output pairs that allow for the efficient pruning of the key space when applying a SAT based attack [20]. An adversary is assumed to have access to a second activated IC, which is used to modify a subset of the applied key bits. The adversary also has complete access to the scan chain of the IC, which allows for the read-out of the internal circuit state.

4 VULNERABILITIES OF INDEPENDENTLY SECURED ANALOG AND DIGITAL CIRCUIT BLOCKS

Research on protecting ICs from a multitude of threats has resulted in methodologies to independently secure analog and digital circuits. In a typical AMS IC pipeline, multiple components of the circuit must be secured against reverse engineering. A discussion on potential vulnerabilities of independently securing the analog and digital blocks is provided in this section. An overview of the AMS pipeline used as an example throughout the paper is described in Section 4.1. A description of the implemented obfuscation technique is provided in Section 4.2. An analysis of an attack to determine the key of the analog and digital circuits through isolation of each block is described in Section 4.3.

4.1 Proposed AMS Circuit Implementation

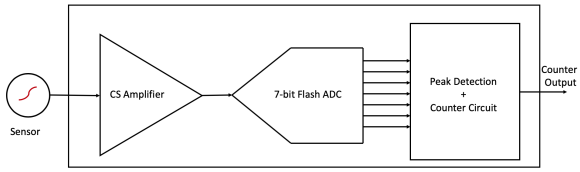

Figure 1: AMS circuit obfuscated with the proposed technique.

A peak detection and counting circuit is considered, which consists of an analog front end, analog-to-digital converter, and digital back end as shown in Fig. 1. The peak detection and counting circuitry is applicable to a wide-range of applications including heart-rate monitoring devices, mass spectrometers, X-ray machines, and image processing applications. The analog front end consists of a common-source amplifier with a diode connected load used in the detection and amplification of a low-voltage output signal from a sensor. The output of the amplifier is applied to a 7-bit flash analog-to-digital converter (ADC). The output of the ADC is connected to a back-end digital computation block comprising of a peak detection circuit and a counter. The two most significant output bits from the ADC, referred to as Bit-1 (B1) and Bit-2 (B2), are applied to the peak detection circuit, where a bit flip from 0 to 1 on B1 implies the detection of a peak over a set threshold voltage and a bit flip from 1 to 0 of B2 returns the circuit to an active detection state.

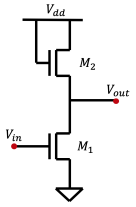

Figure 2: Schematic of the common-source amplifier with diode-connected load.

4.1.1 Common Source Amplifier With Diode-Connected Load. The schematic of the proposed common-source (CS) amplifier is shown in Fig. 2. Due to challenges in fabricating large on-chip resistors that fall within a tight tolerance, diode connected loads are preferred. The gain of the common source amplifier is given by

$$A_v = -\frac{1}{1+\eta}\sqrt{\frac{\left(\frac{W}{L}\right)_1}{\left(\frac{W}{L}\right)_2}}, \tag{1}$$

where η is the back-gate transconductance parameter and $\left(\frac{W}{L}\right)_1$ and $\left(\frac{W}{L}\right)_2$ represent the width over length ratios of transistors M_1 and M_2, respectively. From (1), the amplifier gain is neither a function of the bias current nor the input signal, which results in a linear amplifier gain, tolerance to input and output voltage level fluctuations, a high input resistance, and a high open loop-gain. In addition, the gain of the amplifier is a function of the transistor sizes, which provides a direct design parameter available to obfuscate the amplifier gain. In the proposed obfuscated circuit, the common-source amplifier is designed to produce a gain of 8x when biased by a DC voltage of 0.45 V for an input signal with a peak-to-peak amplitude of no more than 0.04 V.

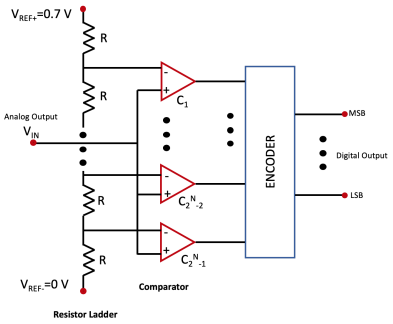

Figure 3: Schematic representation of the flash ADC.

4.1.2 7-Bit Flash Analog-to-Digital Converter. The amplified signal is digitized using a 7-bit flash ADC as shown in Fig. 3. The ADC consists of a 2^N resistive divider providing the reference voltage for the $2^N - 1$ comparators. A logic 1 is produced when the analog voltage is higher than the set reference voltage applied to the comparator. Otherwise the output from the individual comparators is a 0. The combined outputs from all the comparators results in a thermometer code, which is then translated to the appropriate digital output code using an encoder.

4.1.3 Peak Detection and Counting Circuit. The peak detection circuit connected to the output of the ADC is set to a voltage threshold of 0.6125 V, which determines if the most significant bit of the ADC (B1) transitions to a logic *1*. A state machine diagram of the circuit is shown in Fig. 4, where state *S1* signifies the system is waiting for the detection of a peak and *S2* signifies the state of the system once a peak has been detected. The circuit only detects another peak after the voltage falls below a second set threshold (0.525 V for the designed circuit), which is represented by the second most significant bit of the ADC (B2).

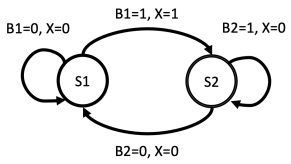

Figure 4: FSM of the peak detection and counting circuit.

Once a peak is detected, the output signal X is used to advance a 3-bit counter. By monitoring the output of the counter, the circuit is able to detect peak bursts or signal abnormalities if a large number of peaks are observed over a bounded period of time.

4.2 Implementation of the Obfuscation Techniques

Obfuscation techniques are implemented on both the analog and digital blocks of the circuit. The 7-bit flash ADC is the only un-obfuscated block of the IC. The parameter obfuscating technique proposed in [13] is applied to the analog circuit with a 10-bit key. The digital circuit is obfuscated with a 6-bit key using a combination of XOR-based logic encryption [5] and stripped functionality logic locking (SFLL) [14]. The total key length applied to the circuit is 16-bits.

4.2.1 Analog Circuit Obfuscation. The gain of the common source amplifier is masked using the vector-based parameter obfuscation technique described in [13]. Parameter obfuscation is a key based technique that targets the physical dimensions of the transistors used to set the optimal biasing conditions of the circuit. The width of a transistor is obfuscated and, based on an applied key sequence, provides a range of potential biasing points. Only when the correct key sequence is applied and certain transistor(s) are active, are the correct biasing conditions at the target node set.

The effective transistor $\frac{W}{L}$ ratio of the diode connected load is masked by using ten diode-connected load transistors each with different sized transistor widths connected in parallel. Each of the ten transistors is either activated or remains deactivated based on a digital key applied through a decryption block implemented using pass transistor logic. From (1), the gain of the CS amplifier is inversely proportional to the square-root of the $\frac{W}{L}$ ratio of transistor M_2. The desired transistor width is only set when the correct key is applied, which produces the target amplifier gain A_v [13].

4.2.2 Digital Circuit Obfuscation. The digital circuitry is obfuscated with two separate techniques. The first is an implementation of XOR based logic locking [5] within the counter of the digital block. The selection strategy for the XOR based locking technique was random and two XOR gates were inserted within the counter circuit. The second technique is applied to the logic cone within the peak detection circuit, where the circuit is modified for a single minterm input. The circuit implemented in [14] that produces a zero Hamming distance from the inputs of the digital block and the applied key is utilized to correct the flipped minterm.

The circuit characterizing the Hamming distance compares four key inputs and four inputs from the peak detection circuit. The four monitored inputs include B1 and B2 from the output of the ADC and the two outputs from the registers of the state machine shown in Fig. 4. The added security of the circuit is, therefore, bounded by 2^4 distinguishing input patterns (DIPs), where the number of DIPs is correlated to the size of the circuit being secured.

4.3 Attacking AMS Blocks in Isolation

The system level schematic shown in Fig. 1 includes a 10-bit key applied to the CS amplifier and a 6-bit key applied to the digital peak detection and counter circuit. When protecting both circuit blocks, the objective is to include obfuscated circuitry that adds to the overall security of the IC, which is bounded by a key space of 2^{16} combinations. However, if not properly implemented, an adversary is able to isolate the analog and digital circuit blocks, which allows for the independent determination of both the key for the CS amplifier and the key for the digital peak detection and counter circuit. Two techniques to isolate the analog and digital blocks are described: 1) using saturating conditions of the analog circuit block (Section 4.3.1) and 2) partially altering the keys of an activated IC (4.3.2).

4.3.1 Saturation Conditions of the Analog Circuit. The CS amplifier of the AMS circuit produces two responses that are known independent of the key. The first response is a result of applying a 0 V input to the CS amplifier. Independent of the applied gain set by the key, the output of the amplifier remains 0.45 V (the DC offset). A logic *0* is produced at the input of the digital circuit for both B1 and B2, which results in the generation of SAT based constraints that more efficiently attack the key space. The second response is due to the saturation of the CS amplifier, which results in an output of 1.8 V, the set power supply voltage (VDD) for the 180 nm technology node used for SPICE simulation. Therefore, applying VDD to the input of the amplifier produces a known output of VDD. DIPs are, therefore, generated for the digital circuit when an all one input is applied to the peak detection circuit. Applying the known logic zero and logic one constraints results in the SAT attack determining the key of the digital circuit in four iterations. Once the digital key is determined, the analog key is now vulnerable to an isolation attack, essentially reducing the key space to 2^{10} combinations from the maximum possible combinations of 2^{16}.

4.3.2 Partial Activated IC by Applying Semi-Correct Key. As part of the threat model described in Section 3, an adversary is assumed to possess access to a second activated IC. The second activated IC allows for partial key modifications, whether applied solely to the digital or analog portions of the circuit. For example, consider an adversary attempting to attack the key of the analog block in isolation. The adversary must determine a set of key values and inputs to the peak detection and counter circuit that exposes the value of the ADC bits (sensitizes the ADC bits). The miter circuit of the AMS circuit shown in Fig. 1 is utilized to determine an input pattern that is dependent on the value of B1 at the output of the digital block. The key inputs and scan chain inputs of the digital circuit are modified and applied to the second activated IC, which allows for the correct determination of the B1 bit based on the input voltage applied to the CS amplifier. The adversary is, therefore, able to set a voltage input to the amplifier that results in the switching of the output of the digital circuit. Inputting a voltage (0 V and VDD) as a constraint to the circuit eliminates all but the correct key, which allows the adversary to decrypt the analog block and reduce the key search space from a maximum of 2^{16} combinations to 2^6.

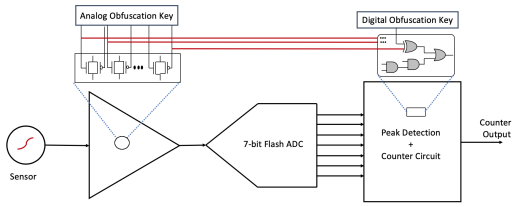

Figure 5: AMS circuit topology with dependencies between the analog and the digital blocks. The key for the digital circuit block is now dependent on the key set for the analog circuit.

The opposite condition also applies, where the adversary simply determines the output of the ADC that isolates the digital portion of the AMS circuit. The adversary applies a SMT solver to determine input and key conditions to the analog block that result in the desired ADC outputs, at which point the activated response of the digital system is obtained. The conventional SAT attack is then executed on the digital block of the circuit. For each determined DIP of the digital block by the SAT solver, the circuit input and key inputs to the analog block are determined such that the target B1 and B2 values are generated. Executing the described attack on the given AMS circuit requires only three iterations of the SAT attack to determine the correct digital key.

5 ADDING KEY DEPENDENCIES BETWEEN ANALOG AND DIGITAL CIRCUIT BLOCKS OF AN AMS CIRCUIT

An attack on a secured AMS circuit that isolates the digital and analog blocks by applying saturating inputs and/or partial key modifications on an activated IC is demonstrated in Section 4. The generation of key dependencies between the AMS circuit blocks is described in this section, which results in an increase in the difficulty of determining the key of an AMS circuit when isolating the digital and analog blocks.

To correlate the key response of the analog and digital circuits, an XOR gate with two key inputs, one from the analog circuit and the other from the digital block, is used. The system model shown in Fig. 1 is now altered to that shown in Fig. 5, with the added correlation between the keys of the analog and digital blocks shown in red dashed lines (interconnects between the analog obfuscation key and digital obfuscation key in Fig. 5).

To implement the interdependence between the analog and digital blocks, four random pairs of analog and digital key bits are chosen and XORed together. By including the correlated keys, the circuit is no longer vulnerable to the attack described in Section 4 that exploits saturating zero and one inputs to trim the key space. Instead, eight valid digital keys remain after the application of the saturating conditions. Essentially, the SAT attack is able to deduce that the analog and digital keys are either equal or inverses of one another, but is not able to determine the value of either key.

Execution of the partial key attack described in Section 4.3.2 no longer results in the determination of the key of the digital block as the output is also dependent on the analog key bits. As an example, consider applying the SAT solver to generate a condition that outputs a value of *1110000* by the ADC. Even though the output of the ADC is known, the generated analog key is also provided to the digital block, which results in a functionally incorrect output from the IC. The adversary is, therefore, forced to concurrently consider the analog and digital blocks of the IC to determine the key.

To attack the linked blocks, the saturating conditions are first applied. The key space is constrained to eight possible digital key values, which reduces the key space from 2^{16} to 2^{13} combinations. A SMT based attack is then applied to the analog portion of the AMS circuit by generating a miter circuit that is inputted to a satisfiability modulo theory (SMT) solver. The SMT solver allows for the mathematical expression of the gain equation of the CS amplifier. Simply applying a miter circuit with analog parameters includes challenges as a floating point value differing by a single least significant bit (LSB) generates an undesired but valid miter circuit constraint. To eliminate a larger set of keys per generated DIP, a range of applied voltages is applied to the activated IC. As an example, consider a DIP generated with an input voltage of approximately 0.0378 V and the internal state registers in the digital block set to *01110*. The saturating conditions of the circuit are first checked for the given internal register state. The circuit switches one of the output register values of the counter for the operating range of the amplifier (less than 0.04 V). Since the output switches based on the applied input to the CS amplifier alone, an adversary knows that the obfuscated gain of the amplifier is vulnerable to attack. To exploit the condition that an applied voltage within the operating input voltage range of the amplifier switches B1 or B2 from a logic *0* to a *1*, the initial input voltage of the DIP (0.0378 V in this example) is varied by ±30% to determine if the logical output of B1 and B2 changes. The ±30% range on either side of the applied input voltage to the ADC generated by the DIP can be constrained more aggressively. A larger range provides a greater probability to observe the change at the output of the circuit, but results in a less constrained key space. A smaller range more effectively constrains the key space, but results in greater difficulty in determining the toggle voltage of B1 and B2. For the implemented peak-detection circuit, three DIPs with a 30% search margin are sufficient to constrain the AMS circuit to return the correct key. The attack on the entire AMS circuit required 12 iterations of the SAT solver, which was substantially greater than the three total iterations required when attacking the analog block in isolation or the four total iterations when independently attacking the digital block.

As AMS circuits require protecting digital and analog IP, an assurance that the added security is not vulnerable to isolation attacks is needed. The proposed method that links the keys of the analog and digital sub-blocks resulted in a significant enhancement of the security of the implemented circuit.

6 SECURING AMS SYSTEMS

The analysis of the security of the AMS peak detection circuit indicates multiple considerations to account for when concurrently securing analog and digital circuit blocks. The following design criteria is provided as a guide to properly secure AMS circuits:

(1) The analog and digital circuit blocks must be evaluated for input-output combinations that are independent of the applied key. For the AMS circuit in this paper, an input voltage of 0 V sensitizes and isolates the digital circuit block as shown

in Section 4.3.1. To avoid such conditions, the generated digital key must account for saturating DIPs, or the AMS circuit must be dependent on the key for all the possible inputs.

(2) Independently securing digital and analog blocks must be avoided. Therefore, a technique is proposed in the paper to link the analog and digital keys. Such dependencies prevent an adversary from extracting circuit information by partially altering the key of an activated IC, which is discussed in Section 4.3.2.

(3) Ensure that the scan chain and internal testing points are inaccessible to adversaries. The AMS pipeline was highly susceptible to attack as every register within the digital block was accessible. The observability of all of the registers permits access to the ADC output, which results in increased isolation of the analog and digital circuit blocks. Obfuscation, or limitation, of the scan chain and testing circuits is needed to prevent an adversary from efficiently determining the key used for logic locking.

7 CONCLUSIONS

This paper proposes a novel obfuscation methodology to protect AMS circuits against IP piracy and theft by implementing logic and performance locking techniques on the digital and analog domains, respectively. Security analysis utilizing a SMT-based attack on an obfuscated peak detection circuit is performed, indicating a vulnerability when independently implementing obfuscating techniques in the analog and digital circuit sub-blocks. Both saturating conditions of the analog block and application of a partial key to an activated IC allow for the determination of the keys for each circuit block in isolation. To force an adversary to concurrently consider the keys of both circuit blocks, the key inputs between the analog and digital blocks are linked. The interconnection of the keys from the two blocks results in a 3x increase in the number of DIPs required to determine the key of the AMS circuit. Accounting for the security of the entire AMS circuit as opposed to the individual circuit blocks is, therefore, critical when designing an AMS system.

ACKNOWLEDGMENTS

This research is supported in part by the Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a, Drexel Ventures Innovation Fund, and the National Science Foundation under Grant CNS-1648878 and Grant CNS-1751032.

REFERENCES

[1] S. Skorobogatov and C. Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 23–40, September 2012.

[2] U.S Department of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," 2010.

[3] 112th Congress, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," May 2012.

[4] IHS Technology Press Release, "Top 5 Most Counterfeited Parts Represent A $169 Billion Potential Challenge for Global Semiconductor Market," April 2012.

[5] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending Piracy of Integrated Circuits," *Computer*, Vol. 43, No. 10, pp. 30–38, October 2010.

[6] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," *IEEE Design and Test of Computers*, Vol. 27, No. 1, pp. 66–75, February 2010.

[7] J. Rajendran, H. Zhang, C. Zhang, G. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault Analysis-Based Logic Encryption," *IEEE Transactions on Computers*, Vol. 64, No. 2, pp. 410–424, February 2015.

[8] R. D. Newbould, D. L. Irby, J. D. Carothers, J. J. Rodriguez, and W. T. Holman., "Mixed Signal Design Watermarking for IP Protection," *Proceedings of the Southwest Symposium on Mixed-Signal Design*, pp. 249–265, January 2003.

[9] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "IP Protection for VLSI Designs Via Watermarking of Routes," *Proceedings of the IEEE International ASIC/SOC Conference*, pp. 406–410, September 2001.

[10] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Pan, "Provably Secure Camouflaging Strategy for IC Protection," *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, pp. 1–8, November 2016.

[11] F. Koushanfar, "Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, pp. 51–63, February 2012.

[12] IHS Markit, "IoT Trend Watch 2018," 2018.

[13] V. V. Rao and I. Savidis, "Protecting Analog Circuits with Parameter Biasing Obfuscation," *Proceedings of the IEEE Latin American Test Symposium (LATS)*, pp. 1–6, March 2017.

[14] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-Secure Logic Locking: From Theory To Practice," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 1601–1618, November 2017.

[15] K. Juretus and I. Savidis, "Reduced Overhead Gate Level Logic Encryption," *Proceedings of the IEEE/ACM Great Lakes Symposium on VLSI*, pp. 15–20, May 2016.

[16] K. Juretus and I. Savidis, "Reducing Logic Encryption Overhead Through Gate Level Key Insertion," *Proceedings of the IEEE International Conference on Circuits and Systems*, pp. 1714–1717, May 2016.

[17] S. Dupuis, P. S. Ba, G. Di Natale, M. L. Flottes, and B. Rouzeyre, "A Novel Hardware Logic Encryption Technique for Thwarting Illegal Overproduction and Hardware Trojans," *Proceeding of the IEEE International On-Line Testing Symposium*, pp. 49–54, July 2014.

[18] M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri, "On Improving the Security of Logic Locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 35, No. 9, pp. 1411–1424, September 2016.

[19] K. Juretus and I. Savidis, "Increasing the SAT Attack Resiliency of In-Cone Logic Locking," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2019.

[20] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the Security of Logic Encryption Algorithms," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 137–143, May 2015.

[21] Y. Xie and A. Srivastava, "Mitigating SAT Attack on Logic Locking," *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 127–146, June 2016.

[22] M. Yasin, B. Mazumdar, J. Rajendran, and O. Sinanoglu, "SARLock: SAT Attack Resistant Logic Locking," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 236–241, May 2016.

[23] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Z. Pan, "Provably Secure Camouflaging Strategy for IC Protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1–14, September 2018.

[24] K. Juretus and I. Savidis, "Time Domain Sequential Locking for Increased Security," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2018.

[25] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal Attacks on Logic Locking and Camouflaging Techniques," *IEEE Transactions on Emerging Topics in Computing*, Vol. 64, No. 9, September 2017.

[26] D. H. K. Hoe, J. Rajendran, and R. Karri, "Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors," *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, pp. 516–521, July 2014.

[27] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu, "Thwarting Analog IC Piracy Via Combinational Locking," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 1–10, October 2017.

[28] V. V. Rao and I. Savidis, "Mesh Based Obfuscation of Analog Circuit Properties," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2019.

[29] V. V. Rao and I. Savidis, "Transistor Sizing for Parameter Obfuscation of Analog Circuits Using Satisfiability Modulo Theory," *Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 102–106, October 2018.

[30] J. Leonhard, M. Yasin, S. Turk, M. T. Nabeel, R. C. Avot M. M. Louërat, O. Sinanoglu H. Aboushady, and H. G. Stratigopoulos, "MixLock: Securing Mixed-Signal Circuits via Logic Locking," *Proceedings of the IEEE Design, Automation Test in Europe Conference Exhibition*, p. PP, March 2019.

[31] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards Provably-secure Analog and Mixed-signal Locking Against Overproduction," *Proceedings of the International Conference on Computer-Aided Design*, pp. 1–8, November 2018.