Reconfigurable Analog Array for Hardware Security

Ziyi Chen
Department of Electrical and Computer Engineering
Drexel University
Philadelphia, PA
Email: ziyi.chen@drexel.edu

Ioannis Savidis
Department of Electrical and Computer Engineering
Drexel University
Philadelphia, PA
Email: isavidis@coe.drexel.edu

2022 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-6654-8485-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISCAS48785.2022.9937490

***Abstract*—In this paper, a novel field-programmable analog array (FPAA) is proposed to secure the intellectual property (IP) of analog and mixed-signal circuits. A obfuscation technique is developed to efficiently mask the topology of both differential mode and single-ended mode analog circuits. The overhead in performance due to the parasitic impedance of the routing switches is analyzed at the internal nodes connected to the programming switches. Advantages of topology obfuscation include the generation of a large search space, an uncorrelated output response, and flexibility in circuit design. The circuits implemented on the FPAA include an op amp with varying loads, a second order biquad filter, a ring-oscillator, and a frequency divider. For circuits requiring a single configurable analog block (CAB) on the FPAA, the 3 dB bandwidth is maintained around 1 GHz, while circuits requiring multiple CABs operate with frequencies between 200 MHz and 1.5 GHz. The security provided by the FPAA fabric is evaluated on both single CAB implementations as well as multi-CAB circuits. Two attack scenarios are considered, a brute force attack and a topology attack. The multi-CAB circuit provides strong security robustness to both attacks with a minimum search space of 2^{26} for the brute force attack and 2^{10} for the topology attack. The FPAA core is implemented in a 65 nm process with an area of 0.1 mm^2.**

I. Introduction

Hardware security has drawn greater attention in recent years due to the continuously expanding use of integrated circuits (ICs) and the urgent need to secure the intellectual property (IP) found within ICs. While logic locking has been implemented on digital circuits to protect against IP piracy and counterfeiting, securing analog circuits remains a challenge due to the sensitivity of the circuits to parasitic capacitance and resistance. Existing efforts on securing analog circuits include obfuscating the bias conditions [1], threshold voltage [2], or transistor sizes [3]–[5] of a circuit.

Although obfuscating certain parameters of an analog IC prevents an attacker from directly using stolen IP, the internal architecture and the functionality of the circuit remain vulnerable to an attacker if a reverse engineering attack [6] is executed to retrieve the raw netlist of the design. In order to mask the topology, a novel obfuscation technique is developed that utilizes a field-programmed analog array (FPAA) to secure the structure of an analog circuit.

Similar to a field-programmable gate array (FPGA), which is programmed to implement different digital logic functions, the FPAA [7], [8] utilizes routing switches to reconfigure the FPAA fabric into various analog circuits. The programmability of the FPAA is due to the flexibility provided by the individual configurable analog blocks (CABs), and the formation of connections between multiple CABs. Therefore, the FPAA allows for the mapping of simple analog modules into a single CAB, while more complex analog circuits are mapped across multiple CABs. The functionality of the FPAA is unknown prior to programming the routing switches, which implies that the FPAA provides the intended specifications only when the correct programming bitstream is applied.

In this paper, the FPAA is proposed to secure analog ICs. Instead of securing the parameters of an analog circuit, the topology of the targeted baseline design is hidden within the fixed structure of the FPAA fabric, where a baseline design is defined as the original analog circuit being mapped onto the FPAA.

The rest of the paper is organized as follows. The methodology to implement the FPAA as a security measure is described in Section II. The security of implementing a single CAB on multi-CAB circuit is discussed in Section III. Some potential threats and attacks on the FPAA are evaluated in Section IV. Concluding remarks are provided in Section V.

II. Implementation of FPAA fabric as a security measure

The proposed FPAA consists of a 6x6 CAB matrix as shown in Fig. 1. A global switch-less interconnect is used to connect between CABs. In addition, seven I/O ports, one in each column of the array, are utilized to provide direct access to the CABs. A global feedback network is included to allow for the implementation of closed loop systems. Through the FPAA, a novel obfuscation technique is proposed to efficiently mask the transistors and topology of a baseline analog circuit. The technique utilizes the structure of the FPAA fabric to obfuscate the topologies of the implemented analog circuits.

The effects on the performance of the implemented circuits due to the routing switches is analyzed by developing parasitic models for different configurations of the fabric. In addition, the trade-off between security and performance is characterized by comparing the circuit specifications of the baseline design of an op amp with a topologically equivalent op amp implemented on the reconfigured FPAA fabric.

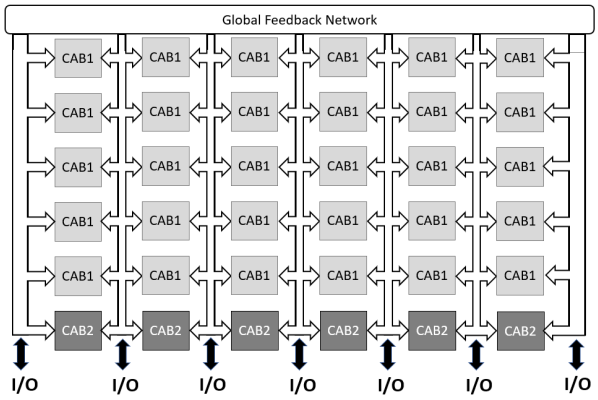


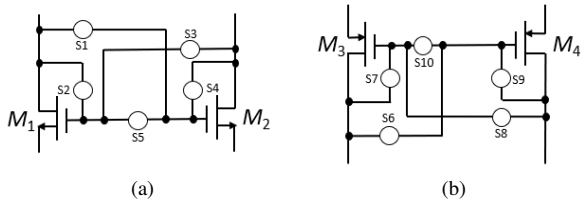
Fig. 1. A FPAA core organized as a 6x6 CAB matrix.

A. Obfuscating the Topology of a Transistor Pair

In order to secure the IP of an analog circuit, a topology obfuscation technique is proposed that masks the connection between two transistors in a generic architecture. As shown in Fig. 2, five switches are utilized to reconfigure the NMOS or PMOS transistor pair into four different circuit topologies, that include a current-mirror, a regeneration loop, a current source, and a diode-connected pair, as shown in Fig. 3. Since differential mode signals are widely used in analog circuits, obfuscating the topology of a transistor pair efficiently secures

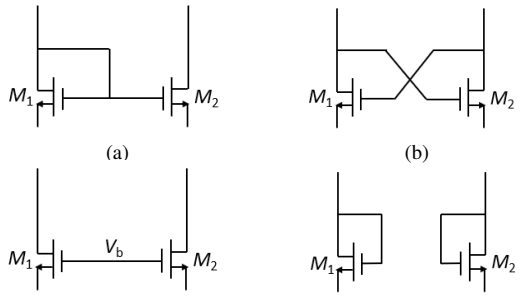
*This work was supported in part by the National Science Foundation under Grant CNS-1751032.

the internal structure of differential mode topologies. Stacking multiple generic transistor pairs allows for the implementation of more complex analog circuits. Single-ended mode circuits are implemented by utilizing half of the transistors of the generic transistor pair.



(a) (b)

Fig. 2. Schematic of reconfigurable (a) NMOS and (b) PMOS pairs.



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

Fig. 3. Possible topologies achieved with a single NMOS transistor pair, which include a (a) current mirror, (b) regeneration loop, (c) current source pair, and (d) diode-connected pair. The same topologies are implemented by the PMOS transistor pair.

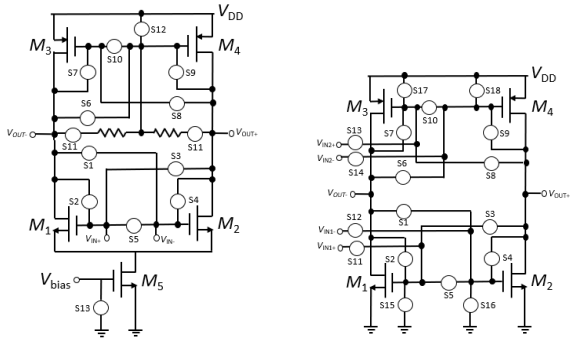
B. CAB Architecture

The architecture of the differential mode CAB (CAB1) is shown in Fig. 4a, where switches S1 to S10 are used to configure the PMOS and NMOS transistor pairs into the four different configurations shown in Fig. 3. The switch S11 is used for common-mode feedback (CMFB), while S12 and S13 are used to turn off the CAB completely. The schematic of a single-ended mode CAB is shown in Fig. 4b, where switches S1 to S10 are used for the configuration of the topology, switches S11 to S14 are used to isolate the input, and switches S15 to S18 turn off the CAB. The programming of an individual CAB into an operational amplifier (op amp) with different loads, a dynamic latch, and a common source amplifier with different loads is provided through Table I, where the ON/OFF state of each switch is listed.

C. Trade-off Between Security and Performance

In this section, the effect on the performance of the CAB due to the routing switches is characterized. The switches allow for fine configuration of each CAB, which provides the FPAA with both greater reconfigurability and security as compared to a fixed circuit topology. However, the routing switches contribute parasitic capacitance to the internal nodes of a circuit, which degrades performance.

To address the effects of the routing switches on the circuit performance, a generic NMOS pair is configured to implement the four different circuits shown in Fig. 3. Utilizing the annotation for switches S1 to S5 shown in Fig. 2, the capacitance C_1 and C_2 shown in Fig. 5 represents the aggregate parasitic capacitance from the drain terminal of switches S1, S2 and S3, S4, respectively. Capacitance C_3 represents the parasitic capacitance from the source terminal of switches S2 and S3, and the drain terminal of S5, while C_4 represents the parasitic capacitance of the source terminal of S1, S4, and S5.



(a) (b)

Fig. 4. Schematic of a (a) differential mode CAB (CAB1), and (b) single-ended mode CAB (CAB2). CAB1 includes 13 routing switches, and in addition to the four possible configurations of the transistor pair, S11 is added to provide common-mode feedback, while S12 and S13 are included to completely turn off CAB1. CAB2 includes 18 routing switches. S11 to S14 are used to isolate both the global switch-less interconnects and the gates of transistors M_1 to M_4. S15 to S18 are used to turn off the CAB.

The on resistance of the corresponding switches is denoted as R_1 to R_5. Due to the parasitic impedances of the switches, the minimum time required to charge or discharge an internal node is longer. The NMOS switches, implemented in a 65 nm process, provide 150 Ω of on-resistance when the *W/L* ratio of the transistor is set to 10 µm/130 nm. The extracted parasitic impedances from the physical layout include 38 fF of capacitance for each of C_1 and C_2, and approximately 41 fF of capacitance for each of C_3 and C_4. Since each CAB contains one reconfigurable NMOS pair and one reconfigurable PMOS pair, the parasitic impedance of the CAB is easily determined based on the configured topology. In addition, the utilization of a switch-less global interconnect network between CABs minimizes the parasitic impedance.

In order to characterize the performance of the CABs, an individual CAB is programmed to implement different analog circuits. Each programmed topology is compared to a baseline design of the circuit, where all the routing switches are removed. The schematic of a differential mode CAB is shown in Fig. 4, with a $(W/L)_{1,2}$ ratio of 80 µm/130 nm and a $(W/L)_{3,4}$ ratio of 98 µm/130 nm.

A comparison of the 3-dB bandwidth between a reconfigured implementation of an amplifier and a baseline design is provided through the results listed in Table II. The post-PEX simulation results indicate a maximum drop in the 3-dB bandwidth of around 3.84 GHz and minimum drop of around 2.3 GHz for the different amplifier topologies listed. The bandwidth for all configurations is greater than 0.8 GHz, although there is a significant drop in the 3-dB bandwidth as compared to the corresponding baseline topology.

III. Security of FPAA fabric

In this section, the security of implementing a circuit on a single CAB and multiple CABs is evaluated. To fully extract a circuit implemented on an FPAA, the attacker must know the location of the activated CAB(s), the configuration of each activated CAB, and the corresponding key for each configured CAB. The security of a circuit implemented on the FPAA is improved by utilizing multiple CABs, as a larger key space and corresponding number of circuit configurations are possible as compared to a single CAB design. The evaluation of the security vulnerabilities is based on attack scenarios with different levels of knowledge of the floorplan, architecture, and configuration principles of the FPAA fabric.

TABLE I
SWITCH CONFIGURATION OF CAB1 AND CAB2 TO IMPLEMENT AN OP AMP, DYNAMIC LATCH, AND CS AMPLIFIER

CAB Type	Configuration Mode		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18
CAB1	Op-Amp	Current Mirror Load	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	ON	OFF	OFF	OFF	-	-	-	-	-
		Current Source Load	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF	-	-	-	-	-
		Current Source Load CMFB	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	ON	OFF	OFF	-	-	-	-	-
		Diode-connected Load	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	ON	OFF	OFF	OFF	OFF	-	-	-	-	-
	Dynamic Latch		OFF	OFF	OFF	OFF	OFF	ON	OFF	ON	OFF	OFF	OFF	OFF	OFF	-	-	-	-	-
CAB2	CS-Amp	PMOS Current Source Load	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF	OFF	ON	OFF	ON
		PMOS Diode-connected Load	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF	ON	OFF	OFF	OFF	OFF	ON	OFF	ON
		NMOS Current Source load	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF	ON	OFF	OFF	OFF	OFF	ON	OFF	ON

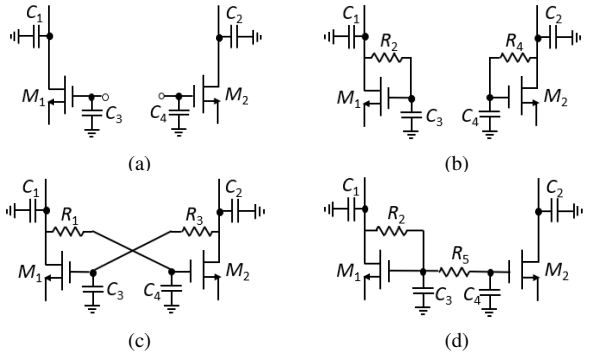


Fig. 5. Parasitic impedance model of an NMOS transistor pair for configurations that include a (a) differential input pair, (b) diode-connected pair, (c) regeneration loop, and (d) current mirror.

TABLE II
3-DB BANDWIDTH COMPARISON BETWEEN THE BASELINE AND RECONFIGURABLE AMPLIFIERS

Implementation		3-dB Bandwidth	
		Reconfigured	Baseline
Op-Amp	Current Mirror Load	887 MHz	3.2 GHz
	Current Source Load	958 MHz	4.8 GHz
	Current Source Load CMFB	1.39 GHz	4.7 GHz

A. Security of a Single CAB

The first attack scenario considers the programming of a single CAB into a target analog circuit, while the rest of the CABs are turned off. Assuming the attacker has no prior knowledge of the FPAA, in order to identify the location of the activated CAB, the attacker must map the structure of the FPAA by delayering and imaging the IC while also gaining access to all I/O ports. If the I/O ports are protected or only one I/O port is available while the FPAA is in test mode, the attacker must then measure the output response of the seven I/O ports while in active mode to identify the location of the activated CAB. However, six CABs within the same column of the CAB matrix share the same input and output port, which implies that the adversary only knows the column in which the CAB is activated by probing the I/O ports. In addition, by activating dummy CABs within other columns of the array, the true location of the targeted CAB is easily obfuscated.

Due to the programmability of the individual CABs, the adversary is not able to easily determine the topology of the baseline design implemented on the FPAA fabric. As shown from the switch configurations listed in Table I, CAB1 is reconfigured into different types of op amps. Since all the op amp configurations amplify the input signal and provide a certain amount of gain, measuring the response at the output does not reveal the internal configuration of the CAB.

The routing switches also prevent the attacker from utilizing the raw unprotected FPAA fabric. Assuming the attacker knows the location of the activated CAB and the specifications of the targeted design, in order to extract the programming keys of the FPAA that implement a target baseline circuit design, the attacker must first access the key bits controlling the gates of the routing switches or delayer the IC and extract the raw netlist of the FPAA through reverse engineering [4]. The FPAA is then treated as a black box, and the attacker measures or simulates the output response with different combinations of the programming key bitstream. The correct programming key is determined when the output response matches the expected specifications of the circuit. Since each CAB1 consists of 13 routing switches, the length of the key for CAB1 is 13 bits. The corresponding search space of finding the key is 2^{13} for a single CAB1 unit when executing a brute force attack. Dissimilar from obfuscating the transistor sizes, where correlation between the key and the output response is utilized by the attacker to reduce the search space [9], the output responses of the randomly programmed CABs remain uncorrelated due to the different types of configured topologies that are possible, as shown from the gain of an amplifier in Fig. 6. The simulated results also indicate that multiple configurations produce similar gains due to keys that result in only slight differences in the implemented topologies. However, other circuit specifications including the DC operating point of each transistor or the feedback conditions differ. The error due to any mismatch in the topologies is also amplified when individual CABs are integrated into a larger circuit. Therefore, an adversary is not able to select a given topology by measuring only one parameter of a programmed circuit. For example, an op amp with or without common mode feedback (CMFB) produces similar gain; however, determining the correct key remains a challenge when other circuit properties or specifications are ignored.

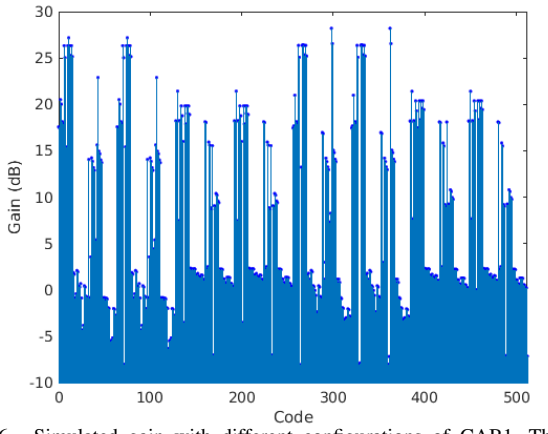


Fig. 6. Simulated gain with different configurations of CAB1. The code represents the binary value of the key bits converted into a decimal number. S3 to S11 are set assuming the attacker knows the location of the CAB, the specifications of the targeted design, and the correct type of input to test the functionality of the circuit.

B. Security of a Multi-CAB System

The implementation of more complex analog circuits is achieved by utilizing multiple CABs distributed in different columns of the array and by using the global feedback network to configure closed loop systems. In order to attack a multi-CAB system, the adversary must first determine the number

TABLE III
IMPLEMENTED MULTI-CAB ANALOG CIRCUITS ON FPAA WITH CORRESPONDING SPECIFICATIONS

Design Name	Num. of CABs	Num. of Output Ports	Key Size	Input Frequency	Output Frequency	Gain
Biquad Filter	4	2	52	$\approx$ 1.5 GHz	$\approx$ 1.5 GHz	-9 to 8 dB
Ring Oscillator	3 to 6	2	39 to 78	-	207 to 478 MHz	-
Frequency Divider	2	4	26	$<$200 MHz	$<$100MHz	-

TABLE IV
THE PROBABILITY OF DECRYPTING THE PROGRAMMING KEYS VIA BRUTE FORCE AND TOPOLOGY ATTACK

Attack Method	Singe-stage Op Amp	Bandpass Filter	Ring Oscillator	Frequency Divider
Brute Force	$\frac{1}{2^{13}}$	$\frac{1}{2^{52}}$	$\frac{1}{2^{36}}$ - $\frac{1}{2^{78}}$	$\frac{1}{2^{26}}$
Topolgy Attack	$\frac{1}{2^{5}}$	$\frac{1}{2^{20}}$	$\frac{1}{2^{15}}$ - $\frac{1}{2^{30}}$	$\frac{1}{2^{10}}$

of CABs being used. As indicated by the circuits listed in Table III, a different number of CABs is required based on the analog circuit being implemented. Even assuming the number of utilized CABs and the location of the CABs distributed in the different columns of the CAB matrix are known by the attacker, the activated CAB (or CABs) in each column is masked by the other CABs of the column.

Implementing a multi-CAB circuit increases the difficulty of determining the functionality of the target analog circuit. In order to determine the functionality of the circuit, the attacker must also know the correct type of inputs to apply. For different analog circuits, the required inputs differ. For example, an amplifier or bandpass filter target input signals with different bandwidths, while a ring-oscillator does not require an input signal at all. The distinct specifications for the different circuits listed in Table III prevent an attacker from inferring the actual implementation of a circuit on the FPAA fabric. Even assuming the attacker determines the location of the activated CAB(s) and the specifications of the targeted design, the larger search space due to the larger number of programming key bits increases the security robustness.

In general, the programmability of the FPAA allows for circuits with significantly differing topologies, functionality, and specifications. Therefore, the target baseline circuit is obfuscated within the large set of topologies possible with the FPAA fabric.

IV. APPLYING ATTACK ON FPAA

In this section, the resilience of the FPAA to two different types of attacks is analyzed, with the assumption that the attacker possesses a certain level of knowledge of the FPAA fabric. The attack scenarios considered include a brute force attack and a topology attack.

A. Brute Force Attack

For a brute force attack, the adversary is assumed to possess access to the key nodes of the routing switches or the netlist of the FPAA fabric. In addition, the attacker must possess knowledge of the complete specification set of the target circuit, the location of the utilized CABs, and the correct output node to observe the response. If such knowledge of the implemented circuit is somehow gained, the attacker must then determine the correct bit stream by feeding in all combinations of programming keys and comparing the output response with the design specifications. The time complexity to solve for the key via brute force attack is exponentially dependent on the key space. The probability to extract circuits implemented on the FPAA fabric through brute force attack is listed in Table IV. In general, the circuit that utilizes a greater number of CABs provides greater robustness against brute force attacks.

B. Topology Attack

Due to the structure of the FPAA fabric, where two transistors are programmed into four different configurations using five routing switches, the key search space is reduced by targeting only the four plausible configurations of the transistor pairs. The pseudocode for executing a topology attack on a single CAB1 is provided as Algorithm 1. In order to correctly determine the key bits that set the routing switches, the attacker must first find all possible configurations of the transistor pair and the corresponding programming keys. A random configuration is then applied to each pair. For the CAB1 architecture shown in Fig. 4a, the configuration of the NMOS transistor pair is chosen first, followed by the configuration of the PMOS transistor pair. If the resulting output matches the oracle output, the corresponding key is considered valid. Consider the CMFB switch, the key space of a single CAB is 2^5. Note, that the attacker is assumed to already know the location of the activated CAB, which implies that the key bits for switches S12 and S13 that are used to turn the CAB on and off are already known and, therefore, ignored. The probability to determine the multi-CAB circuits is also listed in Table IV, which, in addition to ignoring the switches that control the ON/OFF state of the CAB, also assumes that the key bits controlling the feedback network are known.

Algorithm 1: Topology Attack

Input: set of programming switches S = $\{s_1, s_2, ..., s_{13}\}$, pattern switches pair *PS* = $\{(P_1, S_1), (P_2, S_2), ..., (P_4, S_4)\}$;
Output: switch list S_{out};
Find switches connecting to NMOS, PMOS pair; S_P, S_N; // S_P configuring PMOS pair, S_N configuring NMOS pair
for *all* $(P_i, S_i) \in PS$ **do**
  S_P = S_i;
  for *all* $(P_j, S_j) \in PS$ **do**
    S_N = S_j;
    if *circuit_output* = *oracle_output* **then**
      S_{out}.push_back($S_i \cup S_j$)
    end
  end
end

V. CONCLUSIONS

In this paper, the utilization of an FPAA fabric as a security measure is described. A topology obfuscation technique is proposed to efficiently protect both differential mode and single-ended mode analog circuits. The security of implementing single and multi-CAB circuits on the FPAA fabric is evaluated. The implemented circuits include an op amp, a biquad filter, a ring oscillator, and a frequency divider. To attack a circuit implemented on the FPAA, the adversary must locate the activated CAB(s), determine the functionality of the utilized CAB(s), and decrypt the programming keys to configure the FPAA fabric, which is a significant challenge. In addition, a brute force attack and a topology attack are analyzed to evaluate the security of the FPAA, where an assumption is made that the attacker determines the location of the CAB(s) and that the keys that program the global feedback network are known. For a brute force attack, the search space to determine the key is 2^{13} for single CAB design and at least 2^{26} for a multi-CAB design. A multi-CAB implementation of an analog circuit on the FPAA provides robust security with a minimum search space of 2^{10} key combinations for a topology attack and a maximum search space of 2^{78} key combinations for a brute force attack.

REFERENCES

[1] 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, Jul. 2014.

[2] A. A. Saki and S. Ghosh, "How Multi-Threshold Designs Can Protect Analog IPs," *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, pp. 464–471, Oct. 2018.

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

[4] 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, Mar. 2017.

[5] V. V. Rao and I. Savidis, "Performance and Security Analysis of Parameter-Obfuscated Analog Circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 12, pp. 2013–2026, Dec. 2021.

[6] R. Torrance and D. James, "The State-Of-the-Art in Semiconductor Reverse Engineering," *Proceedings of the ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 333–338, Aug. 2011.

[7] J. Becker, F. Henrici, S. Trendelenburg, M. Ortmanns, and Y. Manoli, "A Field-Programmable Analog Array of 55 Digitally Tunable OTAs in a Hexagonal Lattice," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 12, pp. 2759–2768, Dec. 2008.

[8] C. R. Schlottmann and P. E. Hasler, "A Highly Dense, Low Power, Programmable Analog Vector-Matrix Multiplier: The FPAA Implementation," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 1, no. 3, pp. 403–411, Sept. 2011.

[9] V. V. Rao, K. Juretus, and I. Savidis, "Security Vulnerabilities of Obfuscated Analog Circuits," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, Oct. 2020.