Security Vulnerabilities of Obfuscated Analog Circuits

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

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

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

Abstract—**Vulnerabilities of key based analog obfuscation methodologies that modify the transistor dimensions of a circuit are evaluated. Two attack vectors on a common source amplifier, differential amplifier, operational amplifier, and voltage controlled oscillator are developed. The first attack exploits the lack of possible key combinations permitted around the correct key, which is a result of requiring a unique key to lock the circuit. An average of 5 possible key combinations were returned in an average of 5.47 seconds when executing the key spacing attack. The second attack vector utilizes the monotonic relationship between the sizing of the transistors and the functional response of the circuit to determine the correct key. The average time to execute the attack, while assuming process, voltage, and temperature (PVT) variation of 10%, was 1.18 seconds. Both equal key spacing and non-monotonic key dependencies are discussed as ways to mitigate the threats to future analog obfuscation techniques.**

I. Introduction

The demand for analog integrated circuits (ICs) continues to grow while also requiring improved functionality and performance with reductions in power and area. According to a report by Electronic Sourcing, the global analog IC market has shown growth of 4.5% annually from 2017 to 2019 with revenue expected to reach $62.8 billion by 2021 [1]. The growing demand for analog ICs in conjunction with increasing challenges in manufacturing high quality analog circuits in advanced feature sizes has resulted in increased vulnerabilities in the analog IC supply chain. According to a report from ERAI, analog ICs are the third most counterfeited semiconductor component, accounting for 13.36% of the total counterfeits [2]. In addition, companies that produce analog ICs are among the most frequently targeted organizations for counterfeiting [2].

To mitigate the vulnerabilities in the analog IC supply chain, several defensive techniques including split manufacturing, device level obfuscation, logic locking, and key-based analog obfuscation have been proposed. The fundamental principle of the techniques to protect analog circuits is to mask the biasing conditions that set the optimal operating performances of the components. Split manufacturing removes the top metal layers used for interconnect and passive analog components before providing the remaining mask layers of an IC to an untrusted foundry for fabrication [3].

The device level obfuscation techniques proposed in [4] and [5] mask the biasing conditions by changing the device structure and/or properties. A memristor-based voltage divider is implemented in [4] to provide a variable voltage bias to the body of the transistors of a sense amplifier. In [5], nominal V_T (NVT) transistors are camouflaged by replacing the NVT transistors with re-sized low V_T (LVT) or high V_T (HVT) transistors. The sensitivity of analog circuits to process voltage, and temperature (PVT) effects permits the protection of parameters including gain and bandwidth by intentionally manipulating the threshold voltage of the transistors. However, the physical dimensions of the transistors are not protected from an adversary.

The logic locking methodologies described in [6] and [7] obfuscate the digital portion of the mixed-signal IC. Digital circuitry responsible for the post-silicon tuning of the analog circuits is obfuscated using the stripped-functionality logic locking (SFLL) technique described in [6]. The digital section of a $\Sigma\Delta$ analog to digital converter (ADC) comprising of a mixer and a decimation filter is obfuscated in [7].

Key based parameter locking of analog circuits is proposed in [8], [9], and [10], where locking circuitry is inserted into an analog IC to mask the biasing conditions, gains, operating frequencies, and performance parameters. The parameter obfuscation technique proposed in [8] and [9] masks the sizes of the transistors used to set the optimal biasing conditions using parallel (vector) and mesh-based transistor arrays. The current mirror based combinational locking technique proposed in [10] utilizes transistors of different sizes to mask the current gains of the analog circuit. Based on an applied key sequence, a range of currents are set.

In this paper, two attack vectors on key-based obfuscation techniques are proposed that allow for the determination of the sizes of the obfuscated transistors that produce the desired analog circuit performances. The proposed attack vectors motivate the development of the novel analog obfuscation techniques described in this paper as countermeasures.

The paper is organized as follows. Vulnerabilities of current key-based analog performance locking techniques are presented in Section II. An attack vector based on the large difference between the correct and incorrect sizing of obfuscated transistors is described in Section II-B. A second attack vector that leverages the monotonic response of the performance parameters impacted by the obfuscation of different transistors of an analog circuit is provided in Section II-C. Design considerations to prevent the attacks discussed in this paper are presented in Section III. Some concluding remarks are provided in Section IV.

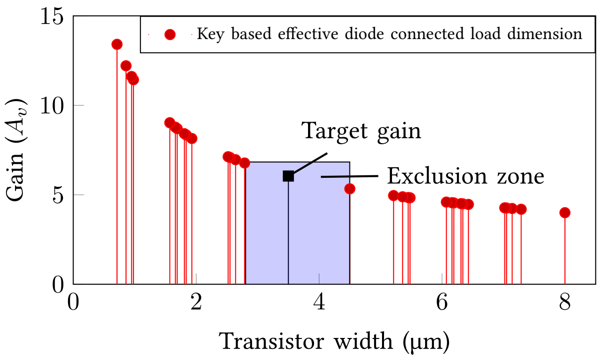

Fig. 1: Effective transistor widths producing corresponding gains when applying different keys to a CS amplifier obfuscated with a 5-bit key.

II. Security Vulnerabilities

Key based performance locking of analog circuits proposed in [8], [9], and [10] target the physical dimensions of the transistors used to set the optimal biasing conditions of the circuit. The width and length of a transistor are obfuscated and based on an applied key sequence to the transistor a range of potential biasing points are set. Only when the correct key sequence is applied, which activates a subset of the composite transistor(s), are the correct biasing conditions at the target node set. Incorrect keys produce effective widths that lead to higher and lower target performance characteristics, such as for the gain, as shown in Fig. 1. The incorrect higher or lower gain results in signal degradation either at the current stage or a future stage of the analog circuit. The two main challenges of implementing parameter biasing obfuscation are 1) the presence of multiple correct keys and 2) the limited deviation in the performance of a circuit when an incorrect key is applied. To mitigate the challenges, a satisfiability modulo theory (SMT) based design methodology has been developed [9], [10] to ensure only a single key produces the correct circuit performance and that an incorrect key results in significant degradation in the operating conditions of the circuit. The formulated problem and the given constraints are provided as inputs to the SMT solver, which outputs transistor sizes that limit the number of correctly functioning keys. The resulting effective widths for a common source (CS) amplifier are shown in Fig. 1.

From the results shown in Fig. 1, two security vulnerabilities are evident, specifically 1) there exists an exclusion zone around the target width where no effective transistor widths are present and 2) the performance parameter has a decreasing monotonic response to the increasing effective width. An increasing monotonic response is also possible dependent on the obfuscated parameter. Two attack methodologies leveraging the observations have been developed as described in this paper.

A. Test Circuits

To evaluate the proposed analog attack methodologies, four analog circuit building blocks are implemented in a 180 nm process and analyzed with SPICE simulation. The building blocks include a voltage controlled oscillator (VCO), common source amplifier with diode connected load, single-stage differential amplifier, and an operational amplifier. The analog circuits are obfuscated with 10, 15, and 20-bit keys, and with 1%, 5%, 10%, 15%, and 20% exclusion zones around the target width. The VCO is designed to operate at 3.25 GHz, where each varactor is obfuscated to mask the operating frequency of the VCO. The common source amplifier is designed to produce a gain of 15 dB, with the diode connected load obfuscated to mask the amplifier gain. The single stage differential amplifier is designed to produce a 30 dB gain and a 4 MHz gain-bandwidth product. The operational amplifier is designed to produce a gain of 60 dB and a gain-bandwidth product of 50 MHz. The differential input transistors of both the operational and differential amplifier circuits are obfuscated to mask the gain and gain-bandwidth.

B. Key Spacing

The threat model considered for the key spacing attack is that of an adversary that possesses the circuit netlist through which the obfuscated transistor sizes are targeted. No oracle response is needed for execution of the attack. The methodology of the key spacing attack is based on the principle that the obfuscated transistors require an exclusion zone around the target device dimension. The psuedocode for the key spacing attack is provided as Algorithm 1. The attack utilizes an SMT solver to determine the active width segments of an obfuscated transistor W based on the key $\vec{X}$, where $\vec{X} \in b[0, 1]$. The nearest width W_a greater than W is determined through execution of an optimization algorithm. If W_a is greater than the specified tolerance value Var, then W is added to the list of candidate keys. The constraints of the model representing the circuit provided to the SMT solver are updated to ensure the next W generated is less than W_i or greater than $W_i + var\_spacing$, where W_i is the candidate key from the previous SMT iteration and $var\_spacing$ is the percentage separation between the given width and the next allowed width (exclusion zone). The previous constraint is valid since any keys within W_i and $W_i + var\_spacing$ do not satisfy the key spacing constraints. As $var\_spacing$ is increased, the number of invalid keys eliminated per iteration increases. The process is repeated until there are no additional satisfying widths.

Algorithm 1: Key Spacing Attack

```
Input: Width Values $\vec{W}_v$,
Key Spacing Variance $Var$;
$W = \vec{W}_v * \vec{X}$;
$S_1 = W \wedge (sum(\vec{X}) > 0)$;
$candidate\_keys = []$;
while SAT[$S_i$] do
    $W_a = find\_adjacent\_width(W_i)$;
    var_spacing = $W_i * Var$;
    if $W_a - W_i >= var\_spacing$ then
        $candidate\_keys.append(W_i)$;
    $S_{i+1} = S_i \wedge (\vec{W}_v < \vec{W}_{v_i} \vee \vec{W}_v > \vec{W}_{v_i} + var\_spacing)$;
end
return candidate_keys;
```

TABLE I: Results of the key spacing attack on a VCO, CS amplifier, differential amplifier, and operational amplifier obfuscated with a 10, 15, and 20-bit key for exclusion zone sizes of 1%, 5%, 10%, 15%, and 20%. The algorithm of the key spacing attack is characterized for the number of candidate keys and the time to determine the candidate solutions.

Circuit Type	Key Size	Exclusion Zone=1%		Exclusion Zone=5%		Exclusion Zone=10%		Exclusion Zone=15%		Exclusion Zone=20%	
		Candidate Keys	Time to Solve (s)	Candidate Keys	Time to Solve (s)	Candidate Keys	Time to Solve (s)	Candidate Keys	Time to Solve (s)	Candidate Keys	Time to Solve (s)
VCO	10	61	4.34	13	1.69	3	0.97	4	0.79	2	0.43
	15	98	12.73	14	10.46	5	6.16	5	0.43	4	2.52
	20	89	487.68	19	71.16	7	68.21	4	71.85	3	72.52
CS Amplifier	10	37	5.62	9	1.35	6	0.96	2	0.68	3	0.47
	15	100	11.39	8	12.11	8	3.21	4	3.80	3	2.86
	20	75	768.38	7	166.14	8	144.47	2	121.89	4	66.23
Differential Amplifier	10	90	1.28	9	1.11	5	1.07	7	0.91	4	0.40
	15	22	92.32	8	15.40	2	7.60	4	2.29	3	1.80
	20	54	671.58	7	367.97	4	101.29	4	64.80	4	48.85
Operational Amplifier	10	67	4.04	11	1.63	5	0.98	4	0.63	2	0.56
	15	35	47.61	21	5.43	5	4.92	5	3.72	4	1.92
	20	36	1520.31	22	88.48	7	100.32	5	117.05	3	89.56

SMT analysis is performed to evaluate the execution of the key spacing attack on a VCO, operational amplifier, differential amplifier, and common source amplifier, with results listed in Table I. The attack is more efficient when the PVT variation is greater, as the number of eliminated keys per iteration increases. The time to solve also increases exponentially as the key size increases, which indicates a less feasible attack for circuits with very large key sizes.

C. Monotonic Circuit Response Attack

The threat model for the monotonic attack assumes an adversary has access to an oracle IC that is utilized as a black-box to obtain input-output responses. The attack makes use of the monotonic relationship between the given width and the output response of the circuit, which applies to a majority of the analog circuit blocks. For example, the monotonic decrease in the gain of a common sources (CS) amplifier as the transistor width is increased is shown in Fig. 1. The monotonic nature of an obfuscated circuit parameter allows an adversary to efficiently partition the keyspace with oracle responses and eliminate any need for modeling the analog circuit with governing equations.

The pseudocode for the monotonic function attack, which prunes the key space, is provided as Algorithm 2. The attack begins by querying an output of the oracle and applying a variation offset to the obtained value to represent any process, voltage, and/or temperature (PVT) variations that alter the output response of the circuit. The SAT constraints are then utilized to select a width, which is applied to the obfuscated transistor. The response from the non-activated IC for the given width is used to analyze the parameter characteristics of the circuit (i.e. gain, bandwidth, and operating frequency). The algorithm checks if the circuit response falls outside of the range of possible values as compared to the oracle response, and if so, constrains the selection of the width during the next iteration of the solver. If the returned response falls within the accepted range of circuit properties, then the given key is added to the list of candidate keys. The process continues until no further widths are generated. The algorithm concludes by returning the list of candidate keys.

The results of executing the monotonic attack on a VCO, operational amplifier, common source amplifier, and a differential amplifier are listed in Table II, which indicate a very effective attack as the key space is cut in half each iteration. For 10% PVT variation, the maximum number of candidate keys returned is 132, which allows an adversary to perform a brute force attack to determine the correct key. The adversary is also able to evaluate the oracle at additional operating conditions and re-execute the attack to further reduce the keyspace. Most of the attacks conclude on the order of a few seconds, with the longest attack requiring approximately one minute to complete, demonstrating a significant vulnerability. In addition, as opposed to the key spacing attack, the attack runtime does not increase significantly with key size since adding additional key bits only linearly increases the number of iterations required by the algorithm to execute.

Algorithm 2: Monotonic Attack

```
Input: Width Values $\vec{W_v}$,
Key Spacing Variance $Var$;
$W = \overrightarrow{W_v} * \overrightarrow{X}$;
$S_1 = W \wedge (sum(\vec{X}) > 0)$;
$candidate\_keys = []$;
$oracle\_response = query\_oracle()$;
$oracle\_min = oracle\_response * (1 - Var)$;
$oracle\_max = oracle\_response * (1 + Var)$;
while SAT[$S_i$] do
    $ckt\_response = get\_circuit\_response(W_i)$;
    if $ckt\_response > oracle\_max$ then
        $S_{i+1} = S_i \wedge (W < W_i)$;
    else if $ckt\_response < oracle\_min$ then
        $S_{i+1} = S_i \wedge (W > W_i)$;
    else
        candidate_keys.append($W_i$);
        $S_{i+1} = S_i \wedge (W \ != W_i)$;
end
return candidate_keys;
```

III. Design Insight

Based on the vulnerabilities of analog circuits to the key spacing and monotonic attacks, two design considerations are proposed to strengthen the security of the existing parameter obfuscation techniques: 1) equal key spacing and 2) obfuscating multiple nodes to create key dependencies that result in a non-monotonic output response. The proposed techniques are compatible with existing SMT based methods used to determine the sizes of transistors to obfuscate [9].

TABLE II: Results from executing a monotonic attack on a VCO, CS amplifier, differential amplifier, and operational amplifier all obfuscated with a 20-bit key. PVT variations of 1%, 5%, 10%, and 20% are analyzed. The algorithm implementing the monotonic attack is characterized for the number of candidate keys, execution time, and the number of iterations of the SMT solver.

Circuit	Exclusion Zone Margin (%)	PVT Variation=1%			PVT Variation=5%			PVT Variation=10%			PVT Variation=20%		
		Candidate Keys	Time to Solve (s)	No. Iter	Candidate Keys	Time to Solve (s)	No. Iter	Candidate Keys	Time to Solve (s)	No. Iter	Candidate Keys	Time to Solve (s)	No. Iter
VCO	1	3	0.57	28	27	1.16	58	71	2.67	101	181	13.84	201
	5	1	0.49	23	5	0.57	28	15	0.83	37	46	2.29	63
	10	1	0.46	19	2	0.44	20	11	0.72	31	35	1.43	55
	15	1	0.42	20	1	0.43	20	7	0.47	22	31	1.56	48
	20	1	0.30	13	1	0.32	13	3	0.39	15	20	0.79	37
CS Amp	1	1	0.45	23	5	0.50	26	9	0.58	31	20	0.73	38
	5	1	0.46	24	1	0.46	24	5	0.48	25	13	0.66	35
	10	1	0.50	25	1	0.51	25	4	0.55	29	24	0.93	47
	15	1	0.49	22	1	0.43	22	2	0.45	23	13	0.70	34
	20	1	0.53	24	1	0.53	24	1	0.53	24	6	0.52	26
Diff Amp	1	4	0.55	16	16	0.80	36	31	0.99	48	71	2.09	98
	5	1	0.45	21	6	0.63	30	46	1.53	67	577	24.76	604
	10	1	0.54	24	8	0.67	33	47	1.44	67	882	50.42	904
	15	1	0.36	15	1	0.33	15	6	0.55	25	19	0.81	40
	20	1	0.32	14	1	0.30	14	5	0.49	5	16	0.73	33
Op Amp	1	5	0.77	34	40	1.33	65	132	3.98	157	900	59.59	926
	5	1	0.52	21	7	0.51	24	18	0.78	36	46	1.56	60
	10	1	0.32	14	3	0.37	17	13	0.82	40	38	1.31	64
	15	1	0.37	18	1	0.40	18	9	0.54	25	27	1.03	45
	20	1	0.45	18	1	0.39	18	3	0.43	20	29	1.01	45

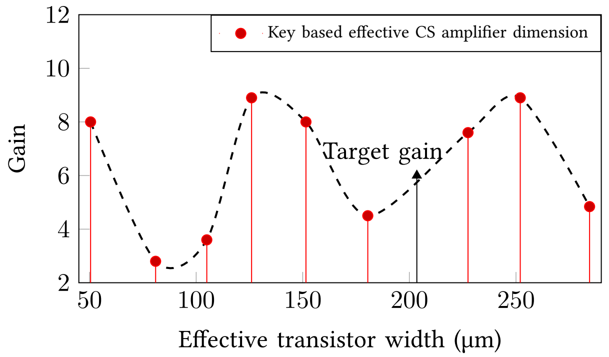

Fig. 2: Effective transistor widths of a CS amplifier with corresponding gain when obfuscated using non-monotonic key dependencies. Both transistors of a CS amplifier are obfuscated resulting in a non-monotonic gain response.

A. Equal Key Spacing

The efficiency of the key spacing attack is dependent on keys existing within the bounds of the margins of the widths of a given key when accounting for PVT variations. For example, if the evaluated width is 5 μm and there are ten widths within a 5% margin, then the attack does not have to consider those 10 widths in subsequent iterations of the execution of the algorithm. However, if the keys produce widths of equal spacing, then the attack requires the same number of iterations as a brute force attack. The width spacing generated by the keys must be considered when obfuscating an analog circuit. The trade-off of using keys that produce equally spaced widths is the additional area required as the widths of the obfuscated transistors are larger. A reduction in area is possible by limiting the widths to generate a desired number of candidate solutions, which results in a trade-off between the efficiency of the attack and the overhead in area when implementing a target security threshold.

B. Creating Non-Monotonic Key Dependencies

The efficiency of the monotonic attack is due to the monotonic relationship of the obfuscated width and the circuit response. If the keys produce a non-monotonic dependency in the functional output response of the circuit, the attack is no longer guaranteed to produce the correct key. To generate non-monotonic dependencies in the function of the circuit, multiple circuit parameters must be concurrently obfuscated. For example, in a CS amplifier, obfuscating both transistors results in a non-monotonic gain as a function of width as shown in Fig. 2. Since the gain is no longer monotonic, the adversary is unable to significantly prune the keyspace when the oracle response does not match the obfuscated circuit response.

IV. Conclusions

Security vulnerabilities based on both the spacing of key values and the monotonic response of the circuit as keys are applied are demonstrated in this paper for key-based analog obfuscation techniques. The key spacing attack utilizes the presence of an exclusion zone around the target transistor size to determine candidate keys without the need of an oracle IC. The monotonic attack utilizes the response of an oracle IC to efficiently partition the keyspace without requiring the adversary to develop circuit equations of the target parameters (gain, bandwidth, frequency) of the obfuscated circuit. The developed attacks were evaluated on a VCO, common source amplifier, differential amplifier, and an operational amplifier for 10, 15, and 20-bit key sizes and for 1%, 5%, 10%, 15%, and 20% exclusion zones around the target width. The results indicate that an average of 5 candidate keys were returned in an average time of 5.47 seconds for the key spacing attack. For the monotonic circuit response attack, the average execution time was 1.18 seconds when assuming 10% PVT variation. Methodologies to thwart the proposed attacks are developed, including equal key spacing and non-monotonic key dependencies, which provide increased security when implementing analog obfuscation.

Acknowledgments

This research is supported in part by the Drexel Ventures Innovation Fund, and the National Science Foundation under Grant CNS-1751032.

References

[1] Electronic Sourcing Online Report, "Rising Demand from Multiple Segments Drive Analog IC Market," July 2018.

[2] ERAI report, "2017 ERAI Reported Parts Analysis," December 2017.

[3] Y. Bi, J. Yuan, and Y. Jin, "Beyond the Interconnections : Split Manufacturing in RF Designs," *Proceedings of the Open Access Journal on Electronics*, pp. 541–564, August 2015.

[4] 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.

[5] A. A. Saki and S. Ghosh, "How Multi-Threshold Designs can Protect Analog IP," *Proceedings of the IEEE Conference on Computer Design (ICCD)*, pp. 464–471, October 2018.

[6] J. Leonhard, M. Yasin, S. Turk, M. T. Nabeel, M. M. Louërat, R. C. Avot, 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*, pp. 7:1–7:8, March 2019.

[7] 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 (ICCAD)*, pp. 1–8, November 2018.

[8] 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.

[9] 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.

[10] 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.