DNA: DC Nodal Analysis Attack for Analog Circuits

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

Kyle Juretus
Villanova University
Villanova, Pennslyvania 19085
Email: kyle.juretus@villanova.edu

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

Abstract*—In recent years, deobfuscation algorithms have been proposed to evaluate the resiliency of analog obfuscation techniques. Each analog deobfuscation algorithm considers different threat models, is applicable to only a small set of obfuscation techniques, and suffers adversely under real world scenarios, where one or more pieces of information on the circuit and obfuscation technique(s) is unavailable to the attacker. In this paper, a novel DC-based nodal analysis (DNA) attack algorithm is proposed that requires only the circuit netlist and the DC input-output response of the oracle IC to perform the attack. The DNA attack utilizes Kirchhoff's voltage law (KVL) and Kirchhoff's current law (KCL) to efficiently characterize an obfuscated analog circuit with the objective of determining the correct obfuscation parameters. A preliminary evaluation of the proposed attack is performed on three distinct analog circuits secured using both key-based parameter obfuscation and a non-key-based multi-threshold obfuscation technique. The results from executing the attack on the analog circuit secured with key-based obfuscation indicate that the attack successfully eliminated 96% of keys from the search space on average for single-stage circuits. The results from executing of the attack on two-stage circuits secured with multi-threshold obfuscation indicate that 99.58% of the keys are eliminated from the search space in less than 7 hours. With the limited information necessary to perform the attack, efficiency in pruning the key-space under real world attack scenarios, and the application of the attack to all the current analog obfuscation techniques, the DNA attack aims to be the de-facto standard to measure the resiliency of analog obfuscated circuits.

***Index Terms*—analog obfuscation, circuit design, SAT, SMT**

I. Introduction

In this paper, a novel DC nodal analysis attack algorithm is proposed to evaluate the strength of different analog obfuscation techniques. Unlike the current state-of-the-art analog deobfuscation techniques [1], [2], [3], the proposed deobfuscation methodology is applicable across threat scenarios and for all existing analog obfuscation techniques. The proposed algorithm only requires knowledge of the circuit netlist and the DC input-output response of the oracle IC.

The paper is organized as follows. Background information on the state-of-the art deobfuscation algorithms and obfuscation methodologies is presented in Section II. A brief discussion on the specifications of the benchmark analog circuits used for evaluation of the attack is provided in Section III. A description of the four different scenarios developed to evaluate the algorithm is provided in Section IV. The DNA attack is described in Section V. The results from the evaluation of the proposed attack algorithms are described in Section VI. Some concluding remarks are provided in Section VII.

II. Previous Works

A brief overview of the key-based parameter obfuscation and multi-threshold obfuscation techniques is provided in this section. In addition, an overview of the current state-of-the-art analog deobfuscation attacks is also described.

A. Analog Obfuscation Techniques

Analog obfuscation techniques fall into two main categories: key-based and non-key-based methods. In this paper, key-based parameter obfuscation and non-key-based multi-threshold obfuscation are selected to evaluate the performance of the DNA attack. The two techniques are selected as both allow for general applicability of obfuscation methodologies to a wide range of threat scenarios and analog circuit types.

For the key-based parameter obfuscation technique proposed in [4], the width and length of a transistor are obfuscated. Only when the correct key sequence is applied are the correct biasing conditions at the target node set that result in the correct circuit functionality. In [5], the use of a fabrication process with multi-threshold voltages (V_{TH}) [5] is proposed to protect analog ICs from reverse engineering. A small number of nominal V_{TH} (NVT) transistors are replaced with low V_{TH} (LVT) and/or high V_{TH} (HVT) transistors, while maintaining the target performance specifications of the circuit.

B. Breaking Analog Obfuscation Techniques

To evaluate the security of the analog obfuscation techniques, four attack methodologies have previously been proposed [1], [2], [3]. In [1], a satisfiability modulo theory (SMT) based algorithm is used to determine the correct key that results in the desired circuit functionality. Generic analog circuit equations are constructed using the circuit netlist, and the SMT algorithm is used to determine the correct key that results in the same circuit performance as that of the oracle IC. In [2], a genetic algorithm (GA) is used to determine the correct key by minimizing the error between the simulated circuit netlist and an oracle IC. The key spacing attack proposed in [3] utilizes an SMT solver to determine candidate widths with sufficient spacing from the next closest widths, which is a potentially exploitable characteristic of key-based

[*] This work was supported in part by the National Science Foundation under Grant CNS-1751032 and the Office of Naval Research under Award N00014-22-1-2071.

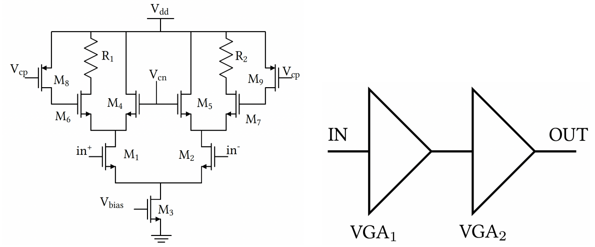
obfuscation techniques. The monotonic attack proposed in [3] utilizes an SMT solver to determine the monotonic relationship between the obfuscated circuit parameter(s) and the output response of the circuit.

III. Circuit Implementations

The three analog circuits that are secured and then used for evaluation of the analog obfuscation attacks are discussed in this section.

A. Variable Gain Amplifier

The circuit schematic of a single stage VGA is shown in Fig. 1a. Two topologies of a VGA are secured utilizing the two obfuscation techniques described in Section II-A, where one topology consists of a single-stage circuit and the other topology consists of two stages. Transistor M_3 of the single stage VGA is secured utilizing the key-based parameter obfuscation technique, which masks both the target output gain of 8.3 dB and the target bandwidth of 100 MHz. The circuit schematic of the two stage VGA is shown in Fig. 1b, where two single stage VGAs are serially connected. A 12-bit key is utilized to mask the total combined gain of the two stage VGA obfuscated using key-based parameter obfuscation.



(a) Single stage VGA (b) Two stage VGA

Fig. 1: Circuit schematic of a (a) single stage VGA and (b) two-stage VGA. Each circuit is secured with key-based parameter obfuscation, where the single stage VGA is obfuscated by a 10-bit key and the two stage VGA is obfuscated by a 12-bit key.

B. Mixer

The circuit schematic of a Gilbert mixer is shown in Fig. 2. The mixer is designed to output a 100 MHz V_{IF} signal and with a conversion gain (CG) of 3.25 dB. The conversion gain of the mixer is masked by obfuscating the dimensions of transistor M_7 with a 10-bit key utilizing key-based parameter obfuscation.

IV. Security Evaluation of Analog Attack Algorithms

In this section, four analog attack scenarios, based on the level of circuit information available to the adversary, are described. In Scenario I, the attacker possesses all circuit information except for the obfuscated parameter(s). For the attack described by Scenario II, in addition to not having the correct key, the attacker no longer possesses the PDK information. For attack Scenario III, the adversary is assumed to no longer possess the biasing information of the circuit in addition to not having the PDK documentation, while attempting to determine the correct key. For attack Scenario IV, the adversary only possesses the oracle IC. As the proposed attack requires the obfuscated circuit netlist, the DNA attack is unable to execute under Scenario IV.

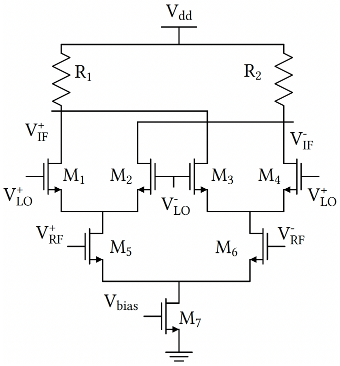


Fig. 2: Circuit schematic of a Gilbert mixer.

V. DC Nodal Analysis (DNA) Attack

The threat scenarios considered for the proposed attack includes access to the obfuscated analog circuit netlist, which is utilized to build a model of the circuit. In addition, access to an oracle IC is needed to determine the analog DC voltages of the inputs and outputs and the overall current of the circuit. The primary objective of the attack is to determine the keys that result in the same output voltage as that of the oracle output when applying the same input to the circuit.

Algorithm 1: DC Nodal Analysis Attack

```
Input: Circuit Model, Width $\vec{W_v}$, $\vec{X} \in b[0,1]$,
       Tolerance $V_{Tol}$, $I_{total}$, $V_{in}$, $V_{oracle_{out}}$;
$W_i = \vec{W_v} \cdot \vec{X}$;
$S_1 = SMTSolver$;
//Device specifications added to S1 model
$S_1 = W \wedge (sum(\vec{X}) > 0)$;
$candidate\_widths = []$;
$oracle\_min = V_{oracle_{out}} \cdot (1 - V_{Tol})$;
$oracle\_max = V_{oracle_{out}} \cdot (1 + V_{Tol})$;
$S_1.add(V_{out} = compute\_output\_voltage(W))$;
$S_1 = S_1 \wedge oracle\_min \leq V_{out} \leq oracle\_max$;
while SAT[$S_i$] do
    candidate_widths.append($W_i$);
    $S_{i+1} = S_i \wedge (W \; != W_i)$;
end
return candidate_widths;
```

Based on the extracted netlist, a simple verilog model is constructed of the obfuscated analog circuit that consists of devices including resistors, capacitors, inductors, and transistors. Basic DC models of the devices are constructed that govern the voltage at internal nodes and the current through given paths, where the inductors are treated as short circuits, capacitors are modelled as open circuits, and the voltages and the currents through the resistors and the transistors are defined by square-law models.

The pseudocode for the DNA attack is provided as Algorithm 1. The input to the algorithm includes the circuit model, the list of obfuscated widths ($\vec{W}_v$), the key-bits ($\vec{X}$) used to set the active widths, user-defined acceptable variation in the computed output voltage V_{Tol} from the SMT solver, the total current of the oracle circuit I_{total}, the input DC voltage V_{in}, and the output voltage of the oracle IC $V_{oracle_{out}}$ for the given input voltage V_{in}. Initially, the SMT solver selects a random key sequence $\vec{X}$ and then determines the active width segment (W_i) of an obfuscated transistor based on $\vec{X}$. The user-specified tolerance V_{Tol} is then used to compute the range of acceptable SMT-computed output voltages, bounded by the minimum voltage $oracle\_min$ and the maximum voltage $oracle\_max$. Based on the inputs, the SMT solver is used to compute the output voltage V_{out}, where the SMT solver propagates the V_{in} voltage to the output node using KCL and KVL equations and the circuit model. Constraints to the SMT solver are added that force a search for widths that result in V_{out} within the range of $oracle\_min$ and $oracle\_max$. If the output voltage is within the user specified tolerance, the selected width W_i is considered as a candidate and constraints are added to determine different keys that meet the target conditions. The SMT solver terminates after exhaustively searching the key-space until *UNSAT* (not satisfiable) conditions are met and returns the list of candidate keys. The attacker then performs a brute-force attack on the returned candidate key list to determine the correct key.

The DNA attack executed on circuits secured with the key-based parameter obfuscation technique is slightly modified for the analysis of the multi-threshold obfuscation technique. The circuit model from the extracted netlist is constructed, where instead of using keys to set the transistor parameters in the evaluation of the key-based parameter obfuscation technique, the keys in the analysis of the multi-threshold obfuscation technique are the selection of process defined threshold voltage V_T for each transistor. Each transistor in the secured analog circuit is obfuscated by a three bit hot encoding corresponding to the three available transistor thresholds $V_{th_{nominal}}$, $V_{th_{high}}$, and $V_{th_{low}}$, where a high bit 1 represents the selection of a particular V_T transistor. The least common bit (LSB) of the three bit encoding is mapped to represent a low threshold transistor, the second bit represents a nominal threshold transistor, and the most significant bit (MSB) represents a high threshold transistor.

VI. Performance of DC Nodal Analysis Attack on Analog Obfuscation Techniques

In this section, the DNA attack is evaluated on both parameter obfuscation and multi-threshold obfuscation and for the three applicable attack scenarios described in Section IV. The evaluation of the analog attacks is performed on a server that includes two 12-core Intel Xeon E5 CPUs and 96 GB of DDR4 memory. The timeout for the execution of the attack is set to 5 days (120 hours). If the set timeout is reached, the execution of the attack is terminated and the candidate keys returned to that point are utilized for the analysis of the attack.

Three different tuning nobs, the variation in V_{th}, β, and V_{out}, provide different degrees of constraint to the attack. Initially, the maximum allowed variation in each of V_{th}, β, and V_{out} is set to 5%. If the correct key is not returned by the solver, the variation in V_{out} is incremented by 5%. If the 5% increase in the variation of V_{out} does not result in a correct key, V_{th} and β variations are then increased by 5%. The cycle of incrementing the variations in the V_{out} followed by the variation in both V_{th} and β is performed until the solver returns the correct key.

For Scenario I, where the attacker possesses all the information except for the correct key, ranges of the threshold voltage V_{th}, β, and the output voltage V_{out} are provided to the solver based on the initial set variation in each parameter centered around the target values provided by the PDK. For Scenarios II and III, where the attacker does not possess the PDK information, ranges for the threshold voltage V_{th} and β are provided to the solver by determining the variations of each centered around generic values of V_{th} and β, respectively. For Scenario III, where the attacker does not possess the biasing information of the circuit, the range of bias voltages is determined by considering the operating voltages of the transistors. For the NMOS transistors the lower bound of the range is set to V_{th} and the upper bound is set to V_{dd}. For the PMOS transistors, the lower bound of the V_{bias} range is set to $-V_{th}$ and the upper bound is set to ground (0 V).

A. Performance Evaluation For Key-based Parameter-Obfuscated Circuits

The DNA attack is executed on the benchmark analog circuits described in Section III and for the three attack scenarios presented in Section IV. For Scenarios II and III, the nominal V_{th_n} and V_{th_p} values are set to 0.4 V and -0.4 V, respectively, and with a variation of 25%. In addition, β_n and β_p are set to 200 $\frac{\mu A}{V^2}$ and 55 $\frac{\mu A}{V^2}$, respectively, and with a variation of 50%.

The results of executing the DNA attack on the three analog circuits are listed in Table I. For the single stage circuits, 97.21% of the keys are eliminated on average from the search space under attack Scenario I with an average execution time of 336.41 seconds. For Scenario II, the proposed attack eliminates, on average 94.33% of the key search space in under 185 seconds. In addition, when considering attack Scenario III, the DNA attack eliminated approximately 43% of the search space in less than 30 minutes after exhaustively executing. For the two-stage circuit obfuscated with a 12-bit key, the attack eliminated 85.4% of the key-space in less than 51 hours under Scenario I. For attack Scenario II and III, the proposed DNA attack eliminated approximately 76% and 64% of the key space, respectively, in less than 74 hours and 83 hours, respectively.

B. Performance Evaluation on Multi-threshold Obfuscation

The DNA attack is executed on the benchmark analog circuits described in Section III and for the three attack scenarios presented in Section IV. As the three analog benchmark circuits are designed and characterized in a TSMC 65 nm PDK. Three different thresholds are available, which include

TABLE I: Results of executing the DNA analysis attack on three analog benchmark circuits obfuscated using the key-based parameter locking technique described in Section III and for the three different scenarios described in Section IV.

Scenarios	Circuits	No. of Keys	Time	V_{th} Variation	β Variation	V_{out} Variation	Comment
I	Mixer (10-bits)	31	154.22 s	5.00%	5.00%	5.00%	Correct Key
	VGA (10-bits)	23	518.59 s	5.00%	5.00%	10.00%	Correct Key
	2-stage VGA (12-bits)	668	181080.32 s	10.00%	10.00%	10.00%	Correct Key
II	Mixer (10-bits)	63	134.45 s	25.00%	50.00%	5.00%	Correct Key
	VGA (10-bits)	53	234.17 s	25.00%	50.00%	10.00%	Correct Key
	2-stage VGA (12-bits)	987	266410. 32 s	25.00%	50.00%	10.00%	Correct Key
III	Mixer (10-bits)	464	889.51 s	25.00%	50.00%	10.00%	Correct Key
	VGA (10-bits)	711	2368.38 s	25.00%	50.00%	10.00%	Correct Key
	2-stage VGA (12-bits)	1489	296287.56 s	25.00%	50.00%	10.00%	Correct Key

TABLE II: Results of executing the DNA attack on three analog benchmark circuits secured using the multi-threshold obfuscation described in Section III and for the three different scenarios described in Section IV. For multi-threshold obfuscation, keys refers to the one hot encoding of the threshold voltage of each transistor.

Scenarios	Circuits	No. of Keys	Time	Vth Variation	Beta Variation	Vout Variation	Comment
I	Mixer	4	65.31 s	10.00%	10.00%	10.00%	Correct Key
	VGA	31	85.19 s	5.00%	5.00%	10.00%	Correct Key
	2-stage VGA	91	1550.34 s	10.00%	10.00%	10.00%	Correct Key
II	Mixer	4	559.79 s	20.00%	50.00%	10.00%	Correct Key
	VGA	44	285.31 s	20.00%	50.00%	10.00%	Correct Key
	2-stage VGA	220	2136.13 s	20.00%	50.00%	10.00%	Correct Key
III	Mixer	4	938.52 s	20.00%	50.00%	10.00%	Correct Key
	VGA	73	322.63 s	20.00%	50.00%	10.00%	Correct Key
	2-stage VGA	243	23418.37 s	20.00%	50.00%	10.00%	Correct Key

a low threshold transistor, a nominal threshold transistor, and a high threshold transistor. The results of executing the DNA attack on the three analog circuits are listed in the Table II.

The attack returned on average 17.5 candidate keys in approximately 75.25 seconds for single-stage circuits when considering attack Scenario I. In addition, the proposed attack eliminated approximately 96% of the search space of unknown threshold voltages for single-stage circuits characterized for Scenario I. Under Scenario II and III, the attack eliminated approximately 88.5% and 82.5% of the search space in under 8 minutes and 11 minutes, respectively. The proposed attack eliminated 99.85% of the search space in under 18 minutes when characterizing two-stage VGA under attack Scenario I. Considering Scenario II, the attack eliminated 99.62% of the keys from the search space in 35.6 minutes. In addition, the attack eliminated 99.58% of the keys in 6.5 hours when considering attack Scenario III.

C. Comparison of Resource Metric With The Current State-of-the-art Analog Deobfuscation Techniques

The resource metric accounts for the time required to initialize the deobfuscation attack [6]. The resource metric of the current analog deobfuscation techniques are listed in Table III. The number of steps needed to determine each of the required information is derived from [6]. The listed data indicates that the proposed DNA attack results in a better resource metric as compared to the equation-based SMT [1] and GA [2] attacks. In addition, the proposed attack results in a higher resource metric as compared to the key-spacing [7] and monotonic response [7] attacks. However, unlike the DNA attack, the key-spacing attack is not applicable to circuits secured with non-key based obfuscation techniques and the monotonic attack is unable to determine the correct key for multi-stage obfuscated circuits, where the circuit response is non-monotonic with respect to the obfuscated parameters [6].

TABLE III: Evaluation of the resource metric for the five analog deobfuscation attacks. A check mark implies needed information. The number of steps to determine all needed information is listed, where each step represents one unit of time [6].

Attack Techniques	Required Information					Resource Metrics (Unit-time)
	Netlist	Biasing Information	Models	PDK Information	Circuit Specifications	
SMT [1]	✓	✓	✓	✓	✓	17
GA [2]	✓	✓	✗	✓	✓	14
Key Spacing [3]	✓	✗	✗	✗	✗	6
Monotonic Attack [3]	✗	✗	✓	✗	✓	4
DNA Attack (This work)	✓	✗	✓	✗	✓	**10**

VII. Conclusions

A novel DC nodal analysis attack is proposed that utilizes the KCL and KVL laws to efficiently explore the obfuscated space and determine the correct control parameters of an obfuscated analog circuit. A preliminary evaluation of the proposed attack is performed on three distinct analog circuits obfuscated using both key-based parameter obfuscation and non-key-based multi-threshold obfuscation. The proposed DNA attack effectively eliminated an average of 96% of keys from the search space for single-stage circuits obfuscated with key-based parameter obfuscation when considering Scenarios I and II. For the two-stage circuit, the attack eliminated 75% of the key space across all three scenarios. For multi-threshold obfuscation, the attack eliminated 99.58% of the search space of possible threshold voltages in less than 7 hours when considering Scenario III for a two-stage circuit. In addition, the proposed attack requires a fewer number of resources to initialize as compared to equation-based SMT and GA attacks. The results of evaluating the DNA attack indicate a capability to determine the correct secured parameters of a circuit obfuscated with key and non-key-based techniques. In addition, the efficiency and the use of the DNA attack for different real-world scenarios validate the applicability of the proposed attack as a standard to evaluate the strength of analog obfuscation techniques.

References

[1] N. G. Jayasankaran, A. S. Borbon, A. Abuellil, E. Sánchez-Sinencio, J. Hu, and J. Rajendran, "Breaking Analog Locking Techniques via Satisfiability Modulo Theories," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 1–10, November 2019.

[2] R.Y. Acharya, S. Chowdhury, F. Ganji, and D. Forte, "Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs Using Genetic Algorithm," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 284–294, March 2020.

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

[4] V. V. Rao and I. Savidis, "Performance and Security Analysis of Parameter-Obfuscated Analog Circuits," *Proceedings of the IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 29, No. 12, pp. 2013–2026, October 2021.

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

[6] V. V. Rao, K. Juretus, and I. Savidis, "Hidden Costs of Analog Deobfuscation Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, , No. 01, pp. 1–14, September 2023.

[7] 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.