# Security Oriented Analog Circuit Design Using Satisfiability Modulo Theory Based Search Space Exploration

Vaibhav Venugopal Rao
ECE Department
Drexel University
Philadelphia, PA 19104
Email: vv85@drexel.edu

Ioannis Savidis
ECE Department
Drexel University
Philadelphia, PA 19104
Email: savidis@coe.drexel.edu

***Abstract*—A technique to enhance the security of analog circuits using Satisfiability Modulo Theory (SMT) based design space exploration is described. The analog satisfiability (aSAT) technique takes as inputs generic circuit equations and performance constraints and, by exhaustively exploring the design space, outputs transistor sizes that satisfy the given constraints. The aSAT methodology is applied to parameter biasing obfuscation, where the width and length of a transistor are obfuscated to mask circuit properties. The proposed methodology was used in the design of a differential amplifier and an operational amplifier, where the widths and lengths determined through aSAT analysis were shown to meet the target circuit specifications. For the operational amplifier, transistor dimensions determined through aSAT analysis for a set of performance constraints were characterized and were found to meet the performance targets, however, there was a 7 MHz reduction in the gain bandwidth product. The simulated results indicate that the developed design methodology achieves a fast and accurate determination of transistor sizes for target specifications.**

***Keywords*—analog EDA; obfuscation; analog circuit security; satisfiability**

## I. Introduction

In recent years, there has been a realization that integrated circuits (IC) are vulnerable to counterfeiting, reverse engineering, over-production, and other types of attack. To address vulnerabilities at the circuit level, several techniques have been developed including logic locking, physically unclonable functions (PUF), hardware metering, reconfigurable logic barriers, digital signatures, and public key cryptosystems [1]. Many of these security techniques have been applied to digital systems. However, current research has not addressed the security of analog integrated circuits. Although analog circuits face similar threats, specifically in counterfeiting, reverse engineering, and overproduction, the design of analog circuits and the attack models differ from digital circuits. Therefore, security techniques and methodologies for digital circuits do not extend directly to analog circuits. In addition, the complexity of the analog circuits increases the challenge of designing and implementing security features.

Parameter obfuscation techniques have previously been proposed for analog IP protection [2]. The proposed technique obfuscates the width of the transistors to mask the biasing conditions of the circuit. Application of a key sequence results in a range of potential biasing points, and only when the correct key is applied, correct functionality of the circuit is achieved. Designing transistor widths that result in only one correct key becomes a challenge since small shifts in physical parameters often cause limited deviation in performance. To overcome such design overhead, a satisfiability modulo theory (SMT) based technique is proposed to automatically determine transistor widths such that only a limited number of keys produce the correct operating conditions.

The primary contribution of this paper is the development of an efficient SMT design space exploration methodology for analog circuits that implements parameter obfuscation. Using the proposed methodology, transistor sizes for a given set of performance constraints are determined. The technique is applied to the design of a differential and an operational amplifier, where parameter obfuscation is implemented to mask the target DC gain and gain bandwidth parameters.

The paper is organized as follows. An overview of the parameter obfuscation technique is provided in Section II. The formulation of the problem and the algorithm using analog satisfiability for design space exploration are described in Section III. Implementation of the proposed technique on a differential and an operational amplifier with transistor widths and lengths obtained through execution of the aSAT solver and validated with SPICE simulation are provided in Section IV. Conclusions are offered in Section V.

## II. Parameter Obfuscation

Parameter obfuscation is a key based technique that targets the physical dimensions of the transistors used to set the optimal biasing conditions. 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.

A typical current biasing circuit is shown in Fig. 1(a). The equivalent obfuscated current biasing circuit is shown in Fig. 1(b), where transistors produce currents that are directly proportional to the combined width of the active transistors from the set of parallel transistors. Only on application of the correct key sequence KEY1 are the proper transistor widths selected and, therefore, the proper currents set. When the correct currents are set, the desired $I_{out}$ is obtained [2].

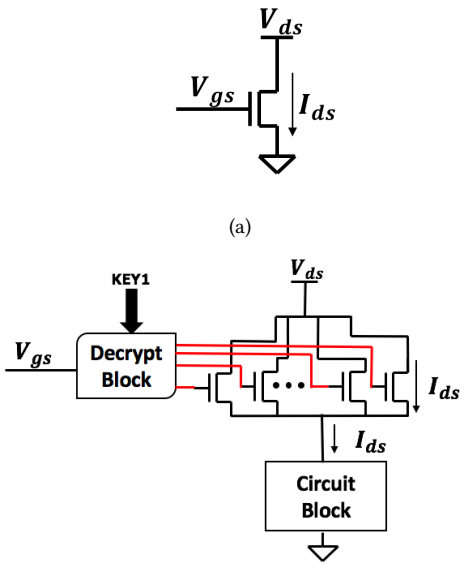


Fig. 1: Current bias circuit that is a) unobfuscated and b) obfuscated.

The technique is applicable to the obfuscation of other width and length dependent circuit parameters including currents, voltages, resistances, capacitances, phase noise, bandwidths, and gains.

## III. Analog Satisfiability (aSAT) for Design Space Exploration

Satisfiability based verification for analog and mixed signal (AMS) circuits has gained significant importance due to the development of powerful SAT solvers. The SAT based techniques provide both the capacity and the efficiency required for solving linear as well as non-linear equations with interval arithmetic constraints [3–6].

### A. *Problem Formulation*

The proposed satisfiability technique uses generic analog circuit design equations such as for gain, operating frequency, phase noise, and bandwidth to determine transistor sizes that meet the given circuit constraints and specifications. The range of widths and lengths along with the circuit constraints are inputs to the aSAT solver. The general formulation of the SAT problem is written as

$$\begin{aligned} X_{min} \leq X \leq X_{max}, \\ Y_{p_{min}} \leq Y_p \leq Y_{p_{max}}, \\ y_j = f(x_i), \end{aligned} \tag{1}$$

where,

- $[X_{min}, X_{max}]$ is the range of transistor sizes,
- $[Y_{p_{min}}, Y_{p_{max}}]$ are the ranges of the circuit constraints,
- $X = \{x_i = 1...n\}$ are the transistor sizes (length and width) for $n$ number of transistors,
- $Y_p = \{y_j = 1...m\}$ are the performance parameters,
- $y_j = f(X), j = 1...n$ are the mapping equations from $X$ to $Y$, and
- $p$ is the index representing each individual constraint.

**Algorithm 1** Width estimation algorithm

**given:**
circuit constraint formulae $\phi$;
$S$= empty solution set;
**while** solution $\neq$ UNSAT **do**
construct interval $[solution - \Delta, solution + \Delta]$;
$S = S \cup [solution - \Delta, solution + \Delta]$;
$\phi = \phi \wedge (x, y) \notin [solution - \Delta, solution + \Delta]$;
Check for Satisfiability;
**end while**
return S;

### B. *SAT algorithm*

The use of SAT to determine the widths of transistors for a given set of analog circuit constraints is described by Algorithm 1. The SAT solver begins by choosing a random width and performance range $(X, Y)$ for each circuit node with interval $[solution - \Delta, solution + \Delta]$. Guidance constraints $(x, y) \notin [solution - \Delta, solution + \Delta]$ are added, which force the algorithm to search for solutions beyond the interval. If a new solution is found by the SAT solver, the solution is used to construct new performance and guidance intervals that include the satisfied conditions from the current guidance interval. The step of updating the performance ranges and guidance interval is continued until the solver returns *UNSAT*. The union of all the intervals is the superset of the solution space.

The primary objective of the parameter space exploration algorithm is to determine a feasible performance space and transistor operating range for the given constraints and specifications. The cost of solving SMT based circuit equations increases exponentially with increasing constraints or with wider parameter ranges. Large dimensions lead to a large initial performance space, which is computationally expensive to search. To address the increased computational cost, the large ranges (transistor dimensions) are sub-divided into smaller ranges. The aSAT algorithm is then applied to each individual sub-space. The benefit of sub-dividing the design space is that each sub-domain is run independently and in parallel, which decreases the computational time.

The two primary challenges of parameter biasing obfuscation are 1) multiple correct keys (multiple widths that produce the desired circuit response) and 2) the limited deviation in performance for incorrect keys. The challenges

TABLE I: Circuit parameter equations for an operational amplifier.

| Circuit Parameter | Dependent Parameters | Governing Equation |
|---|---|---|
| DC Gain | Transconductance | $g_m = \sqrt{2\mu_n C_{ox} W/L * I_D}$ |
| | Output Conductance | $g_{ds} = 1/2 * \mu_n C_{ox} W/L * (V_{gs} - V_t)^2 * \lambda_n$ |
| | First Stage Gain | $\frac{g_{m_2}}{g_{ds_2}+g_{ds_4}}$ |
| | Second Stage Gain | $\frac{g_{m_7}}{g_{ds_7}+g_{ds_8}}$ |
| | Total DC Stage Gain | $A_{DC} = \frac{g_{m_2}}{g_{ds_2}*g_{ds_4}} * \frac{g_{m_7}}{g_{ds_7}+g_{ds_8}}$ |
| Phase Margin | Gain Bandwith | $GBW = \frac{g_{m_1}}{2\pi C_c}$ |
| | Zero (Transfer Function) | $z = \frac{g_{m_7}}{C_c}$ |
| | First Pole (Transfer Function) | $P_1 = \frac{1}{g_{m7} R_1 R_2 C_c}$ |
| | Second Pole (Transfer Function) | $P_2 = \frac{g_{m7}}{C_1+C_2}$ |
| | Phase Margin | $PM = 180 - tan^-1(\frac{GBW}{Z}) - tan^-1(\frac{GBW}{P_1}) - tan^-1(\frac{GBW}{P_2})$ |

TABLE II: W/L ratios determined by applying aSAT to a differential amplifier for a target gain of 40 dB.

| **Parameter** | **Range of W/L Ratio** | **Selected W/L Ratio** |
|---|---|---|
| M1, M2 | [1, 1000] | 6.58 |
| M3, M4 | [1, 1000] | 84 |
| M5, M6 | [1, 1000] | 5.75 |

TABLE III: Comparision of transistor dimensions determined through aSAT with SPICE simulation for different performance metrics.

| **Performance Metrics** | **aSAT target Value** | **SPICE Value** |
|---|---|---|
| $A_v$(dB) | 40 | 35 |
| GBW (MHz) | 5 | 4.4 |
| Power Dissipation ( µW) | $\leq 100$ | 90 |

are addressed through aSAT analysis by sub-dividing the entire design space and by setting the precision of the performance range as an additional constraint. The SAT solver is forced to output all the transistor dimensions that fall within the targeted performance range, which are a discrete set of points in the design space. The widths of the obfuscated transistors are selected such that only one combination of widths represents the solution point, while the remaining combinations fall outside the solution range, ensuring that only a limited number of keys produce the target performance specifications.

## IV. Applying aSAT for Transistor Sizing

To highlight the adaptability of the aSAT algorithm in solving constraint driven equations, the proposed aSAT design methodology is applied to a differential amplifier and an operational amplifier. All parameter selections based on aSAT solutions are obtained using iSAT3 [7]. The widths and lengths obtained from the aSAT solver are then validated through SPICE simulation using a 180nm CMOS process.

### A. Application of aSAT to a Differential Amplifier

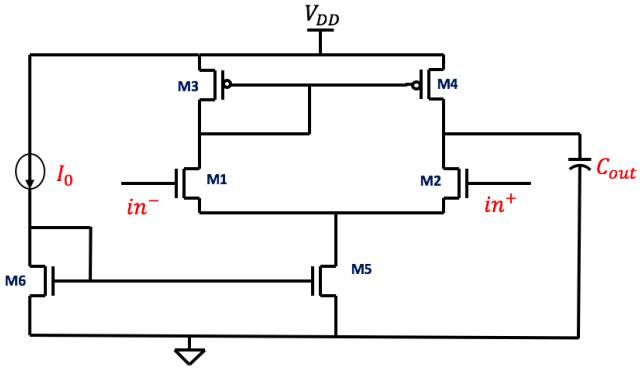


Fig. 2: Circuit diagram of a differential amplifier.

The differential amplifier topology considered in this paper is shown in Fig. 2. Using the equations listed in Table I as circuit constraints, the problem is formulated and inputted into the aSAT solver. The transistor sizes (W/L ratio) determined through execution of the aSAT solver for a differential amplifier with a gain of 40 dB, gain bandwidth of 5 MHz, slew rate of $5V/\mu m^2$, load capacitance $C_{out}$ of 10 pF, input common mode voltage range of 0.8 V to 1.6 V, and power dissipation of less than 100 µW are listed in Table II. The differential amplifier with transistor sizes obtained from the aSAT solver is then characterized with SPICE simulation, and the resulting performance metrics are compared against target circuit specifications. The results of the comparison are listed in Table III.

### B. Application of aSAT to an Operational Amplifier

The topology of the implemented operational amplifier is shown in Fig. 3. The supply voltage $V_{dd}$ is set to 1.8 V and the load capacitance $C_{out}$ is set to 2 pF. The input common mode voltage range is set between 0.8 V and 1.6 V to ensure the transistors remain in saturation. To ensure the stability of the circuit and in order to maintain the phase margin requirements, $C_c$ is set to the smallest value greater than $0.22C_{out}$. Using the equations listed in Table I, while considering additional parameters including input common mode range (ICMR), slew rate, and power dissipation with transistors constrained to operate in saturation, the problem is formulated (circuit constraint equations) and inputted into the aSAT solver. The transistor sizes (W/L ratio) determined through the execution of the aSAT solver for an operational amplifier with a gain of 60 dB, gain bandwidth of 30 MHz, and power dissipation of less than 300 µW are listed in Table IV. The operational amplifier with transistor lengths and widths determined through aSAT analysis is then characterized with SPICE simulation. The performance metrics of the simulated operational amplifier are compared against targeted circuit specifications, with the results of the comparison listed in Table V. The results of the SPICE simulation indicate that the gain, phase margin, and power dissipation constraints are all within the targeted specifications. However, there is a 7 MHz drop in the gain bandwidth product of the amplifier.

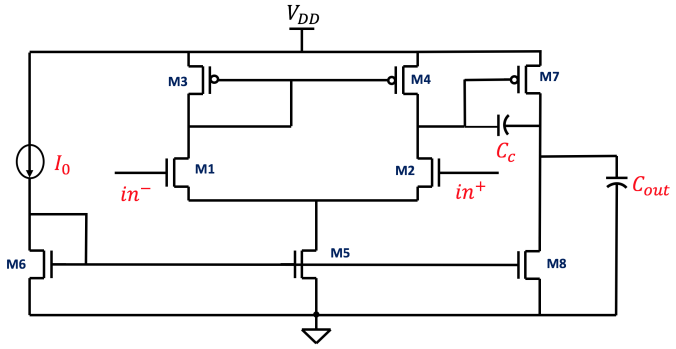


Fig. 3: Circuit diagram of an operational amplifier.

The transistor widths as a function of transistor lengths for the performance specifications listed in column 2 of Table V and the W/L ratios obtained from Table IV are plotted in Fig. 4. By setting the transistor length to a specific value, only a limited set of widths for transistors M1 through M6 exist that meet the target specifications. The obfuscated transistor sizes are set such that only one combination produces the desired circuit operation for a selected length, as shown in Fig. 4.

## V. Conclusions

A novel security oriented analog circuit design methodology is described. The aSAT algorithm provides topology independent results as generic analog circuit equations are solved. The aSAT algorithm was implemented on a differential amplifier and an operational amplifier to determine the transistor dimensions that satisfy the specified performance constraints. For the operational amplifier, the W/L transistor ratios determined through aSAT analysis were found to meet the gain, phase margin, and power consumption requirements of the circuit, but a reduction of 7 MHz in gain bandwidth was observed. The simulated results indicate that the aSAT methodology is an accurate technique to reduce design time for analog circuits that include obfuscated transistors for security.

TABLE IV: Determined W/L ratio when applying aSAT to a operational amplifier for 60 dB gain.

| Parameter | Range of W/L Ratio | Selected W/L Ratio |
|---|---|---|
| M1, M2 | $[1, 1000]$ | 3.62 |
| M3, M4 | $[1, 1000]$ | 7.81 |
| M5, M6 | $[1, 1000]$ | 7.41 |
| M7 | $[1, 1000]$ | 117.81 |
| M8 | $[1, 1000]$ | 55.88 |

TABLE V: Accuracy of transistor dimensions determined through aSAT for different performance metrics.

| Performance Metrics | aSAT target Value | SPICE Value |
|---|---|---|
| $A_v$(dB) | 60 | 63.02 |
| GBW (MHz) | 30 | 23 |
| Phase Margin (°) | $40° \geq PM \geq 60°$ | 49.77° |
| Power Dissipation ( µW) | $\leq 300$ | 206.8 |


## Acknowledgments

This research is supported in part by Drexel Ventures Innovation Funds and the National Science Foundation under Grant CNS-1648878.


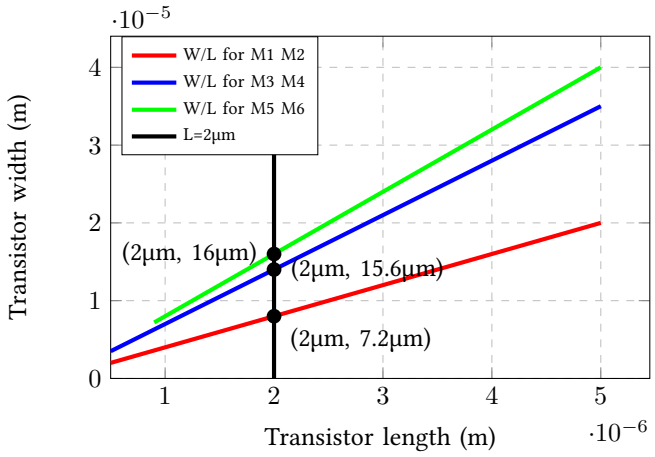


Fig. 4: Widths are selected for transistors M1 through M6 as a function of transistor length. The W/L ratios are selected to meet the circuit constraints given in Table. V.

## References


[1] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1283–1295, August 2014.

[2] 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.

[3] R. Mukul, A. Biere, and A. Gupta, "A Survey of Recent Advances in SAT-Based Formal Verification," *Proceedings of the International Journal on Software Tools for Technology Transfer*, pp. 156–173, April 2005.

[4] R. Mukherjee, M. Purandare, R. Polig, and D. Kroening, "Formal Techniques for Effective Co-verification of Hardware/Software Co-designs," *Proceedings of the ACM Annual Design Automation Conference (DAC)*, pp. 1–6, June 2017.

[5] Y. Deng, "SAT Based Verification for Analog and Mixed Signal Circuits," *Masters Thesis, Texas A&M University*, pp. 1–65, 2012.

[6] O. Lahiouel, M.H. Zaki, and S. Tahar, "Towards Enhancing Analog Circuits Sizing Using SMT-Based Techniques," *Proceedings of the ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, June 2015.

[7] K. Scheibler, S. Kupferschmid, and B. Becker, "Recent Improvements in the SMT Solver iSAT," *Proceedings of the Methods and Description Languages for the Modeling and Verification of Circuits and Systems Conference*, pp. 231–241, March 2013.