2018 IEEE Asia Pacific Conference on Circuits and Systems

Transistor Sizing for Parameter Obfuscation of Analog Circuits Using Satisfiability Modulo Theory

Vaibhav Venugopal Rao
Department of Electrical and Computer Engineering
Drexel University, Philadelphia, USA
vv85@drexel.edu

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

***Abstract*—In this paper, an approach is described for enhancing the security of analog circuits using Satisfiability Modulo Theory (SMT) based design space exploration. The 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 analog satisfiability (aSAT) methodology is applied to parameter biasing obfuscation, where the width of a transistor is obfuscated to mask circuit properties, while also limiting the number of keys that produce the target performance requirements. The proposed methodology is used in the design of a differential amplifier and a two stage amplifier. The widths determined through aSAT analysis are shown to meet the gain, phase margin, and power consumption requirements for both a differential amplifier and a two-stage amplifier. However, a 7 MHz offset in the gain-bandwidth of the two-stage amplifier is observed from the target value of 30 MHz. The total gain of the two stage amplifier is masked with a 24 bit encryption key that results in a probability of 5.96×10^{-08} to determine the correct key. The simulated results indicate that the proposed analog design methodology quickly and accurately determines transistor sizes for target specifications, while also accounting for obfuscation of analog circuit parameters.**

I. Introduction

To address the growing need for analog IP protection, parameter obfuscation techniques have been previously proposed [1], where the width and length of the transistors are obfuscated to mask the biasing conditions of the circuit. Unlike digital circuits, where a single bit error results in a logical failure, a small error in analog circuits often causes a limited deviation in performance. Therefore, determining transistor widths that result in only one correct key becomes a challenge, which leads to increased design time and costs. To overcome such design overhead, a technique based on satisfiability modulo theory (SMT) is proposed for design space exploration to automatically determine transistor widths such that only a limited number of keys produce the correct operating conditions. The proposed technique results in fast and accurate design of analog circuits that include obfuscated transistor sizes for security.

The primary contribution of this paper is the development of an efficient SMT design space exploration methodology for analog circuits that implement parameter obfuscation. The proposed methodology is used to determine transistor sizes for a given set of performance constraints and transistor dimensional bounds (i.e a range of valid transistor widths and lengths). The transistor sizing technique is applied to the design of both a differential amplifier and a two stage amplifier. The parameter obfuscation technique is applied to the two stage amplifier to mask the gain and gain-bandwidth.

An overview of the parameter obfuscation technique is provided in Section II. The problem formulation and the SMT based aSAT algorithm are described in Section III. Application of the aSAT algorithm to determine transistor sizes for the target circuit specifications is discussed in Section IV, and the application of the aSAT algorithm to determine the obfuscated transistor sizes that produce a limited number of functioning keys is described in Section V. Conclusions are offered in Section VI.

II. Background

Parameter obfuscation is a key based technique that targets the physical dimensions of the transistors used to set the optimal biasing conditions of the circuit. The width and length of a transistor are 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.

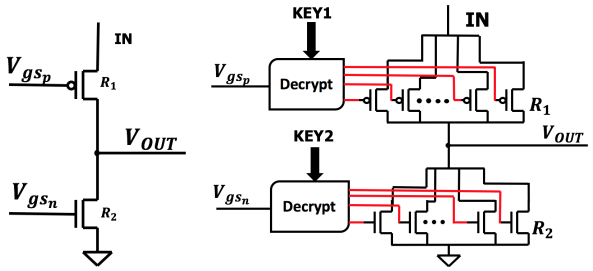
A typical voltage biasing circuit is shown in Fig. 1(a). For the obfuscated biasing circuit, the resulting output resistances are directly proportional to the combined width of the active transistors from the set of parallel transistors comprising the obfuscated devices of the original biasing circuit, as shown in Fig. 1(b). Only on application of the correct key sequences KEY1 and KEY2 are the proper transistor widths selected and, therefore, the proper resistances set. When the correct resistances are set, the desired V_{out} is obtained [1]. The technique is applicable to the obfuscation of other width and length dependent circuit parameters including currents, capacitance, phase noise, bandwidths, frequencies, 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

This research is supported in part by Drexel Ventures Innovation Funds and in part by the National Science Foundation under Grants CNS-1648878 and CNS-1751032.

978-1-5386-8239-5/18/$31.00 ©2018 IEEE



(a) (b)

Fig. 1: Voltage bias circuit that is a) un-obfuscated and b) obfuscated.

the development of powerful SAT solvers. The SAT based techniques provide both the capacity and the efficiency required to solve linear as well as non-linear equations with interval arithmetic constraints [2–5].

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 [6]. 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 dimensions,
- $[Y_{p_{min}}, Y_{p_{max}}]$ 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 m number of 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.

B. *SAT algorithm*

The use of SMT to determine the widths of transistors for a given set of analog circuit constraints is described by Algorithm 1. The constraint formula ϕ is an input to the SMT solver along with technology dependent parameters. The satisfiability of a circuit topology using an SMT solver begins by first selecting a random width and performance range (X, Y) for each circuit node along with the corresponding interval range in the decision process. The SMT solver selects one of the unassigned variables and splits the interval of the variable into two subintervals of the same length. The solver temporarily discards one of the subintervals and reduces the range of the selected interval. The interval constraint propagation (ICP) technique is then applied to ϕ. If the ICP routine terminates with no conflict, then the algorithm

Algorithm 1: aSAT for transistor size optimization

Input: circuit constraint formulae ϕ
Output: S
S=empty set
while *variable with interval greater than* δ *exists* **do**
  decision *()*
    pick the variable and divide the range in half
    select one of the subintervals
  deduction *()*
    if $ICP(\phi)$=*UNSAT* **then**
      find conflict-source s
      $S = S \cup s$
      if *S=entire state space* **then**
        return UNSAT
      else
        undo all decision and deduction after s
        ϕ=$\phi \cap \overline{s}$
      end if
  end if
end while
return *UNSAT*

returns to the decision step. If a conflict exists in the interval due to a reduction of a variable to null, the source of the decision that lead to the conflict is located by the conflict driven clause learning (CDCL) algorithm. When the union of conflict sources covers the entire search space, the algorithm returns UNSAT. Otherwise, a backtrack routine is called and the algorithm returns to the decision process after adding a conflict clause to ϕ. The union of all the intervals is the superset of the solution space.

C. *Application to parameter biasing obfuscation*

The two main challenges that arise in parameter biasing obfuscation are 1) multiple correct keys (multiple widths and lengths that produce the desired circuit response) and 2) the limited deviation in the performance of a circuit when an incorrect key is applied. The challenges are addressed through aSAT analysis by 1) formulating an SMT problem based on the optimized transistor widths that meet the desired circuit specifications, 2) accounting for the number of obfuscated transistors, and 3) accounting for the permitted range of transistor sizes. The constraints for the SMT problem limit the number of effective widths close to the target width, which are set by the applied key. The formulated SMT problem and the given constraints are provided as inputs to the aSAT solver, which then outputs the transistor sizes that limit the number of correctly functioning keys.

IV. Applying aSAT for Transistor Sizing To Meet Circuit Constraints

The proposed aSAT design methodology is applied to a differential amplifier and a two stage amplifier. All parameter

TABLE I: Circuit parameter equations for a differential and two stage 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)	$P_1 = \frac{1}{g_{m_7} R_1 R_2 C_c}$
	Second pole (transfer function)	$P_2 = \frac{g_{m_7}}{C_1+C_2}$
	Phase margin	$PM = 180 - tan\ \ 1(\frac{GBW}{Z}) - tan\ \ 1(\frac{GBW}{P_1}) - tan\ \ 1(\frac{GBW}{P_2})$

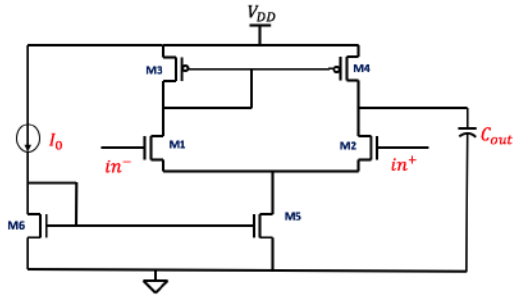


Fig. 2: Circuit diagram of a differential amplifier.

TABLE II: Determined W/L ratios when applying aSAT to a differential amplifier for 40 dB gain. The length for all transistors is set to 1 µm.

Transistor	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

selections based on aSAT solutions are obtained using iSAT3 [7], which is a satisfiability checker for Boolean combinations of arithmetic constraints for both real and integer valued variables. iSAT3 is capable of solving linear, non-linear arithmetic, and transcendental functions. The widths and lengths obtained from the aSAT solver are then validated through SPICE simulation of the amplifier in a 180nm CMOS process.

A. Applying aSAT for Transistor Sizing of a Differential Amplifier

The differential amplifier topology considered in this paper is shown in Fig. 2. To highlight the adaptability of the aSAT algorithm in solving constraint driven equations, ranges of transistor widths and lengths are inputted into the aSAT solver. The algorithm exhaustively and simultaneously explores both transistor width and length ranges and outputs transistor dimensions that satisfy the performance constraints. 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/µm^2, load capacitance C_{out} of 10 pF, input common mode voltage range between 0.8 V to 1.6 V, and power dissipation of less than 100 µW are listed in Table II.

TABLE III: Results from SPICE simulation characterizing the performance metrics of a differential amplifier using transistor dimensions determined through aSAT.

Performance Metrics	aSAT target Value	SPICE Value
A_v(dB)	40	35
GBW (MHz)	5	4.4
Power dissipation (µW)	≤ 100	90

The differential amplifier with transistor sizes obtained from the aSAT solver are 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. The simulated results indicate that all the design constraints including the gain, gain bandwidth, and power dissipation were within 15% of the target values. Further improvement in the accuracy of the aSAT determined transistor sizes is possible by including parasitic models of the circuit as additional constraints.

B. Applying aSAT for Transistor Sizing of a Two Stage Amplifier

The two stage amplifier topology shown in Fig. 3 is considered. 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 operate in saturation. To ensure the stability of the circuit and to maintain the required phase margin, C_c is set to the smallest value greater than $0.22C_{out}$. Applying the circuit equations for a two stage amplifier (listed in Table. I), while setting target values for additional parameters including the input common mode range (ICMR), slew rate, and power dissipation for transistors constrained to operate in saturation, the problem is formulated (circuit constraint equations) and inputted into the aSAT solver. The resulting transistor sizes (W/L ratio) generated by the aSAT solver for the two stage amplifier given a performance target of 60 dB gain, 30 MHz gain-bandwidth, and power dissipation of

TABLE IV: Determined W/L ratios when applying aSAT to a two stage amplifier for 60 dB gain. The length for all transistors is set to 1 µm.

Transistors	Range of W/L ratio	Selected W/L ratio
M1, M2	[1, 1000]	3.2
M3, M4	[1, 1000]	7.81
M5, M6	[1, 1000]	7.41
M7	[1, 1000]	165.22
M8	[1, 1000]	70.84

TABLE V: Results from SPICE simulation of a two-stage amplifier using transistor dimensions determined through aSAT to characterize target 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)	≤ 300	206.8

less than 300 µW are listed in Table IV. The transistor sizes obtained from the aSAT solver are then characterized with SPICE simulation. The performance metrics of the simulated two stage amplifier with widths determined through aSAT analysis are compared against target circuit specifications. The results of the comparison are listed in Table V. The simulated results 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 of the amplifier.

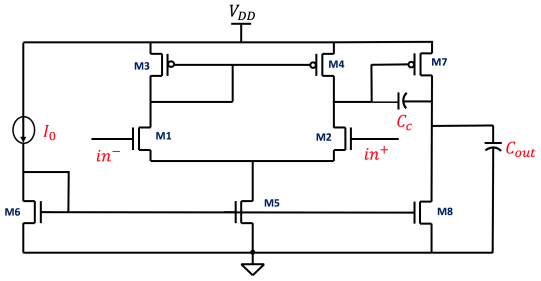
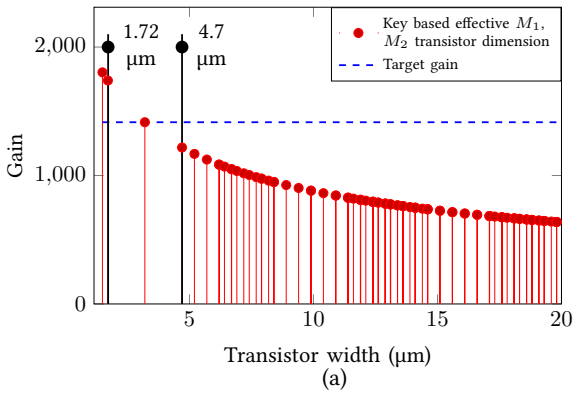


Fig. 3: Circuit diagram of a two stage amplifier.

V. Applying aSAT to Determine Transistor Sizes of the Two Stage Amplifier that Result in a Unique Key

The parameter obfuscation technique is applied to the two stage amplifier circuit shown in Fig. 3. Each of M_1 and M_2 is obfuscated using a seven parallel transistor topology, while M_8 is obfuscated using 10 parallel transistors. Therefore, the two stage amplifier is obfuscated using a 24-bit key that masks the gain and gain-bandwidth parameters. Obfuscation of M_1 and M_2 masks the first-stage gain and gain-bandwidth, while the obfuscation of M_8 masks the second-stage gain of the amplifier.



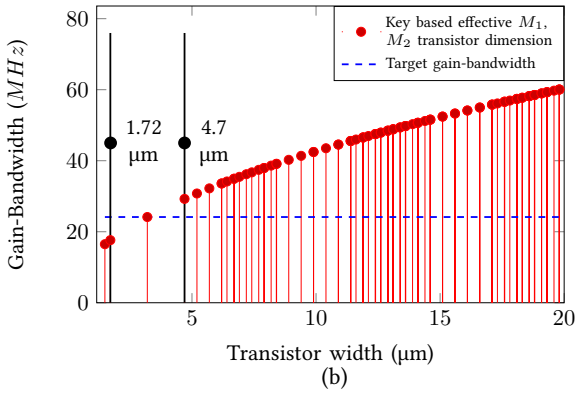


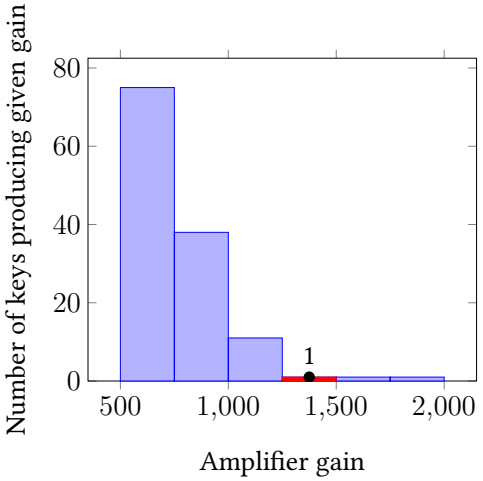
Fig. 4: Effective transistor widths set by a key with the corresponding a) gain and b) gain-bandwidth when transistors M_1 and M_2 of the two stage amplifier are obfuscated. The two widths listed in the figure represent the +/- 40% deviation from the target width.

Analysis was performed characterizing both the gain and gain-bandwidth with respect to the applied keys, and therefore effective transistor widths, with results plotted in Figs. 4a and 4b, respectively. The results shown in Fig. 4 verify that only one key exists that produces the target width, and therefore, the desired gain of 63 dB (1415x), while all other keys result in widths that produce at least 14% variation (2 dB) in gain. Although the next closest incorrect key produces only a 2 dB deviation in the gain, there is also a deviation of at least 20% in the gain-bandwidth. In addition, the target gain and gain-bandwidth are not the individually optimized values. As seen from Fig. 4, the gain and the gain-bandwidth parameters are inversely related as a function of width. The result is an increase in the difficulty of an attacker determining the transistor widths that properly set the gain and gain-bandwidth as the keys produce either higher gain but lower gain-bandwidth or lower gain but higher gain-bandwidth.

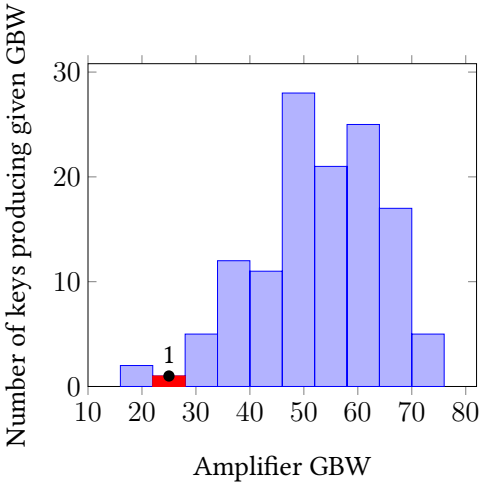
The obfuscated two stage amplifier is characterized by applying all key combinations (seven key bits for M_1 and M_2), with results shown in Fig. 5. The histograms indicate that there exists only one key sequence that results in the desired 63 dB (1415x) gain and 23 MHz gain-bandwidth, which fall within the target range of 62 dB (1250x) to 63.5 dB (1500x) and 22 MHz to 28 MHz, respectively. The above analysis indicates that the aSAT solver generates a limited

number of keys within a small range of the target gain and gain bandwidth, which better masks both the first-stage gain and gain-bandwidth.

Obfuscation of M_8 with 10 parallel transistors masks the second stage gain. The total gain of the amplifier as a function of the width of M_8 is shown in Fig. 6. Applying the aSAT design methodology, transistor sizes are determined such that an incorrect key results in a transistor width that varies by at least 20% of the target width, and therefore, results in at least a 4 dB (37%) degradation of the amplifier gain. The proposed two stage amplifier obfuscated using a 24-bit key results in an 80% overhead in area. However, the probability of determining the correct key is $5.96\text{x}10^{-08}$, which secures the amplifier design from reverse engineering and IP theft.



(a)



(b)

Fig. 5: Histogram of a) gains and b) gain-bandwidths for a two stage amplifier with applied key sequences, where transistors M_1 and M_2 are obfuscated using seven parallel transistors each.

VI. Conclusions

An SMT based aSAT algorithm is proposed to reduce the design time of analog circuits while implementing parameter obfuscation. The aSAT algorithm is applied to a differential amplifier and a two stage amplifier to determine the transistor dimensions that satisfy the specified performance constraints while also meeting the constraints imposed by implementation of the parameter obfuscation technique. For the differential amplifier and the two stage amplifier, the W/L transistor ratios determined through aSAT analysis met the gain, phase margin, and power consumption requirements of the circuit. However, for the two-stage amplifier, a reduction of 7 MHz in the gain-bandwidth was observed.

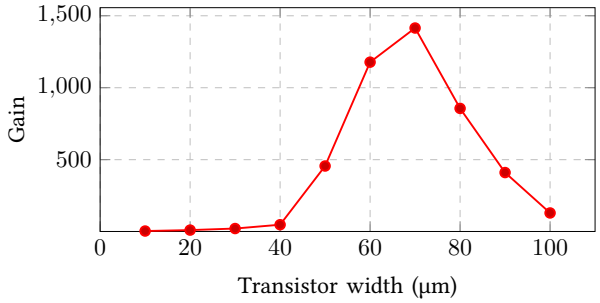


Fig. 6: Analysis of the width of M_8 on the gain of the amplifier.

A novel security oriented analog design methodology, specifically parameter based obfuscation, is implemented on a two stage amplifier that is secured with a 24 bit key. The aSAT algorithm is applied to automatically determine obfuscated transistor sizes for the two stage amplifier such that only a limited number of keys produce the correct operating conditions. The implementation of the parameter obfuscation technique along with the transistor sizes generated by the aSAT resulted in an 80% increase in area. Since only one key produces the correct circuit functionality, the probability to determine the correct key is $5.96\text{x}10^{-08}$. The novel methodologies described in the paper reduce the time to design analog circuits while also securing against IC theft, reverse engineering, and counterfeiting.

References

[1] 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.

[2] 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.

[3] 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. 35:1–35:6, June 2017.

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

[5] 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.

[6] V. V. Rao and I. Savidis, "Security Oriented Analog Circuit Design Using Satisfiability Modulo Theory Based Search Space Exploration," *Proceedings of the 50th Government Microcircuit Application and Critical Technology Conference (GOMACTech)*, pp. 770–774, March 2018.

[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.