Mesh Based Obfuscation of Analog Circuit Properties

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, a technique to design analog circuits with enhanced security is described. The proposed key based obfuscation technique uses a mesh topology to obfuscate the physical dimensions and the threshold voltage of the transistor. To mitigate the additional overhead of implementing the obfuscated circuitry, a satisfiability modulo theory (SMT) based algorithm is proposed to auto-determine the sizes of the transistors selected for obfuscation such that only a limited set of key values produce the correct circuit functionality. The proposed algorithm and the obfuscation methodology is implemented on an LC tank voltage-controlled oscillator (VCO). The operating frequency of the VCO is masked with a 24-bit encryption key applied to a 2x6 mesh structure that obfuscates the dimensions of each varactor transistor. The probability of determining the correct key is 5.96×10^{-8} through brute force attack. The dimensions of the obfuscated transistors determined by the analog satisfiability (aSAT) algorithm result in at least a 15%, 3%, and 13% deviation in, respectively, the effective transistor dimensions, target frequency, and voltage amplitude when an incorrect key is applied to the VCO. In addition, only one key produces the desired frequency and properly sets the overall performance specifications of the VCO. The simulated results indicate that the proposed design methodology, which quickly and accurately determines the transistor sizes for obfuscation, produces the target specifications and provides protection for analog circuits against IP piracy and reverse engineering.**

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

I. Introduction

To address the growing need for analog IP protection, two obfuscation techniques have been previously proposed [1, 2]. In [1], the width of the transistors is obfuscated to mask the biasing conditions of an analog circuit. Based on an applied key sequence, a range of potential biasing points are set. Without proper design considerations, the technique is susceptible to multiple correct keys and potentially provides limited degradation in the functionality of the circuit for a subset of incorrect keys [2]. For the current mirror based combinational locking technique proposed in [2], transistors of different sizes are implemented to mask the current gains of an analog circuit. Based on the applied key sequence, a current is set from a range of possible values. A satisfiability modulo theory (SMT) based algorithm is applied to generate a unique key. The primary disadvantage of the current mirror based combinational locking technique is that unlike the parameter obfuscation technique in [1], which obfuscates the voltages, currents, or gains of an analog circuit with transistor level techniques, the combinational locking proposed in [2] only masks the currents through circuit level techniques (i.e. current mirrors).

The proposed obfuscation technique described in this paper implements a mesh based transistor array to mask the dimensions and threshold voltage of the transistors that set the biasing conditions of the circuit. To reduce the additional overhead required to implement the obfuscation technique and to produce only a limited number of correctly functioning keys, a satisfiability modulo theory (SMT) based technique is proposed for design space exploration to automatically determine the optimal transistor sizes that mask the target functionality of the analog circuit. The proposed methodology provides a means to quickly and accurately design a secure analog circuit. The primary contributions of this paper include

1) the development of a novel mesh based obfuscation technique to secure analog intellectual property (IP) by obfuscating biasing conditions, and
2) the development of a transistor sizing methodology that accounts for the obfuscation technique, resulting in a single key that produces the correct functionality.

The rest of the paper is organized as follows: A discussion on the assumed threat model is provided in Section II. An overview of the mesh based obfuscation technique is described in Section III. The results and analysis of implementing the mesh based obfuscation technique on an LC tank VCO are provided in Section IV. The aSAT algorithm used to determine the obfuscated transistor sizes that produce a limited number of functioning keys is described in Section V. Some concluding remarks are provided in Section VI.

II. Threat Model

An untrusted foundry model is assumed, where the foundry has access to the design of the IC and possesses the necessary tools and skills to counterfeit and overproduce the IC from the provided GDS-II file [3]. In addition, the circuit is assumed trusted and devoid of any malicious components when in the design phase.

978-1-7281-0397-6/19/$31.00 ©2019 IEEE

An additional threat model considered is an untrusted end user. Advances in imaging tools and delayering processes provide the means to reverse engineer and steal circuit IP with features less than 50 nanometers in dimension [4].

III. Mesh Based Obfuscation of Transistor Features

The proposed mesh based topology is shown in Fig. 1, where a single transistor is replaced by a mesh structure. Each transistor in the mesh is of different size and is controlled by a key bit. Based on the applied key bits, certain transistors in the mesh are turned on, resulting in an overall effective transistor length and width. As the effective transistor dimensions vary based on the applied key, the biasing points of the circuit are tunable. The correct biasing conditions are set only on the application of the correct key, resulting in the desired performance parameters.

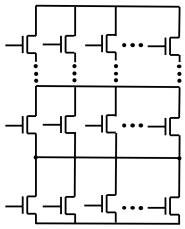


Fig. 1: Mesh topology utilized to implement the proposed obfuscation technique.

The advantage of implementing the mesh based topology is that, in addition to masking the size of the transistors, additional parameters of the circuit including the threshold voltage are easily obfuscated. In addition, due to the series connection of transistors that constitute the mesh, the transistors closest to nominal V_{dd} (top row at higher potential) operate in saturation while the transistors closest to ground (bottom row at lowest potential) operate in linear or sub-threshold mode, which results in the obfuscation of small signal parameters.

A. Obfuscation of Transistor Sizes with a Mesh

The proposed mesh based topology obfuscates both the transistor widths and lengths. Adding transistors in parallel leads to an increase in the overall transistor width while keeping the length constant. The effective width for transistors connected in parallel is given as

$$\left(\frac{W}{L}\right)_{eff} = \frac{W_1}{L} + \frac{W_2}{L} + \frac{W_3}{L} + ... + \frac{W_n}{L}, \tag{1}$$

where $(W/L)_{eff}$ is the effective transistor width over length ratio of n number of parallel transistors.

The series connection of the transistors, as shown in Fig. 1, results in a composite structure where the effective transistor length increases. The schematic of a series connected composite transistor is shown in Fig. 2. For the composite transistor to function properly, M_2 must be larger than M_1

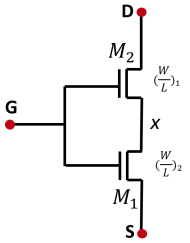


Fig. 2: Equivalent schematic of a 2 row by 1 column series connected composite transistor.

and must operate in saturation, whereas M_1 must operate in linear mode. The current through M_1 and M_2 is given as

$$i_{comp} = \frac{1}{2}\frac{\beta_2\beta_1}{\beta_2+\beta_1}(V_{GS} - V_X - V_T)^2, \tag{2}$$

where β is the product of the electron mobility μ, oxide capacitance C_{ox}, and the transistor width over length ratio (W/L), V_{GS} is the gate to source voltage of M2, V_x is the voltage at node X between transistors M1 and M2, and V_T is the threshold voltage of M2. Based on (2), the effective width over length ratio of the composite transistor is given as

$$\left(\frac{W}{L}\right)_{eff} = \frac{\left(\frac{W}{L}\right)_2\left(\frac{W}{L}\right)_1}{\left(\frac{W}{L}\right)_2 + \left(\frac{W}{L}\right)_1}. \tag{3}$$

B. Obfuscation of Threshold Voltage with the Mesh Topology

In process nodes above 0.25 µm, the threshold voltage is independent of the channel length and channel width [5]. In process nodes below 0.25 µm, the threshold voltage V_T varies due to two effects: 1) roll-off of V_T with decreasing transistor length (short channel effect) [6], and 2) roll-up of V_T with decreasing transistor width (narrow-channel effect) [7]. Based on the applied key, the effective width and length of the composite transistor varies, which results in changes to the threshold voltage. The obfuscation of the threshold voltage allows for the masking of the small signal parameters of the transistor, including the output impedance, gain, and transconductance.

IV. Implementation Of Mesh Based Obfuscation on a VCO

The proposed mesh based parameter obfuscation technique is implemented on a VCO, which is shown in Fig. 3. The dominant biasing parameter of the VCO selected for obfuscation is the size of the varactor transistors as the output frequency of the VCO is highly dependent on the dimensions of the varactor. Therefore, by implementing the mesh based obfuscation technique on the varactor transistors, the target output frequency of the VCO is masked.

The un-obfuscated and obfuscated VCOs are designed in a 180 nm CMOS process. The target operating frequency of the VCO is set to 3.25 GHz. The active transistor area of the VCO-based PLL increases by 145% from 3314 µm^2 to

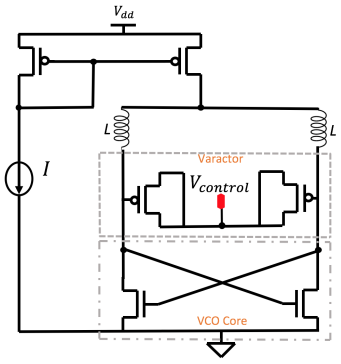


Fig. 3: Circuit schematic of a LC VCO.

8129 μm^2 when accounting for the additional transistors and the key-delivery circuit required to obfuscate the VCO. In a majority of mixed-signal ICs, analog components constitute approximately 2% of the devices present in the circuit and 20% of the total area [8], with the VCO occupying a sub-area of the analog blocks. Assuming a 1 mm × 1 mm IC, the un-obfuscated and obfuscated VCO occupy 0.33% and 0.81% of the total area, respectively. The length of the applied key for the obfuscated circuit is 24 bits. The probability of obtaining the correct frequency of the VCO through brute force attack is, therefore, 5.96x10^{-8}. The proposed mesh based obfuscation technique provides increased security as compared to the vector based obfuscation proposed in [1] and the current mirror based encryption proposed in [2]. The attacker now has to determine not only the correct transistor dimensions but also the threshold voltage and the region of operation (accumulation, depletion, or inversion) of each obfuscated transistor due to the masking of the small signal parameters. The comparison of critical parameters of an obfuscated and un-obfuscated VCO are listed in Table I. Due to the structure of the composite transistor, the overall leakage current is reduced, resulting in an improvement in the phase noise at 1 MHz and 1 kHz.

TABLE I: Characterization of an obfuscated and unobfuscated VCO.

Parameter	**Unobfuscated VCO**	**Obfuscated VCO**
Locking Frequency	3.25 GHz	3.255 GHz
Area of PLL	3314 (μm)^2	8129 (μm)^2
Settling Time	3.9 ns	4.2 ns
Power	18.13 mW	20.72 mW
Phase noise @1MHz	-112.2 dBc/Hz	-116.4 dBc/Hz
Phase noise @1kHz	-38.52 dBc/Hz	-44.46 dBc/Hz

V. Applying aSAT to Determine Transistor Sizes That Result in a Unique Key

To mitigate the design challenges of implementing the proposed obfuscation technique, an aSAT based transistor sizing algorithm is proposed. The fundamental component of the aSAT solver is the satisfiability modulo theory (SMT) based search space exploration algorithm that utilizes iSAT3 [9] [10–13]. By implementing the methodology proposed in [14], the SMT problem is constructed using the target transistor sizes assigned to the mesh, the mesh dimensions (*M*x*N* transistors), and the range of permitted sizes for the obfuscation transistors, along with the composite transistor model described in Section III. The constraints provided to the SMT problem limit the number of effective widths close to the target width.

Algorithm 1: aSAT for obfuscation transistor size optimization

Input: circuit constraint formulae ϕ
Output: S
S=empty set
while *unassigned ObfusTran with interval greater than* δ *exists* **do**
  decision *()*
    assign ObfusTran to the mesh and divide the range in half
    select one of the subintervals
  deduction *()*
    CombFirst=combination(1^{st} row mesh values)
    SumFirst=sum(CombFirst)
    CombSec=combination(2^{nd} row mesh values)
    SumSecond=sum(CombSec)
    EffectiveWidth=apply Eqn. 3
    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*

In Algorithm 1, the formula ϕ consisting of the SMT problem and the given constraints are provided as input to the SMT solver. The SMT solver begins by selecting a random obfuscated transistor in the mesh and splitting the range of dimensions into two subintervals of equal length. The solver then temporarily discards one of the subintervals and reduces the selected interval. The interval constraint propagation (ICP) technique is then applied to ϕ, where the ICP technique determines whether only one target size exists in the *EffectiveWidth* parameter, while all other transistor combinations produce sizes that are smaller or larger than 15% of the target dimensions. If the ICP routine terminates with no conflict, then the algorithm returns to the decision step and selects a different obfuscation transistor until all transistor sizes in the mesh are determined. If a conflict exists, indicated by a reduction of the interval of the range

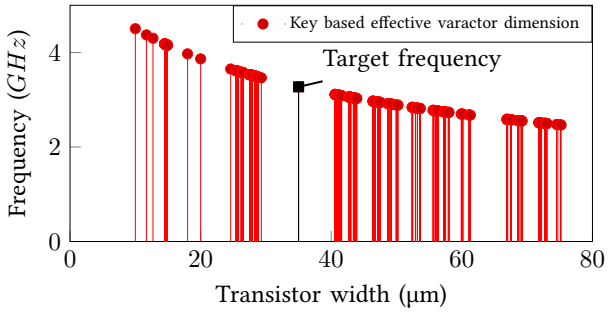
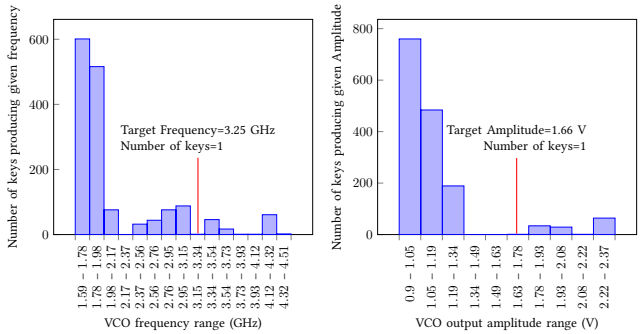


Fig. 4: Effective transistor widths producing a corresponding frequency when different keys are applied to the varactor of a VCO obfuscated by a 2x6 mesh.



(a) (b)

Fig. 5: Histogram of the number of keys that produce binned values of (a) frequency and (b) amplitude when implementing a 2x6 mesh based obfuscation of the varactor of a VCO.

of the obfuscation transistor sizes to null, the source of the decision that lead to the conflict is located by a 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 intervals is the superset of the solution space.

A. Simulation Results

The aSAT solver is utilized to determine the sizes of the varactor transistors each obfuscated by a 2x6 mesh. The target frequency of the VCO is set to 3.25 GHz with an expected output voltage of 1.66 V. Analysis is performed to characterize the total number of keys that produce a frequency and amplitude within binned values. The resulting frequencies, when applying different keys to the 2x6 mesh, are provided in Fig. 4. The results shown in Fig. 4 indicate that only one key produces the target 35 μm varactor width, while all other keys produce transistor sizes that are offset by at least 15% from the target dimensions.

Characterization of the obfuscated VCO is completed for all key combinations, with results provided in Fig. 5. The histogram plot shown in Fig. 5(a) indicates that only one key exists that produces a frequency in the range of 3.15 GHz to 3.35 GHz. In addition, only one key produces an amplitude between 1.34 V and 1.78 V as shown in Fig. 5(b). Although the resulting deviation in frequency when applying an incorrect key is only 3% (or greater) than that of the frequency produced by the correct key, the correct key alone provides the desired amplitude. All other keys produce amplitudes greater than 1.8 V or less than 1.34 V, which, when accounting for all cases, results in at least a 2 dB degradation in the phase noise and a 6% increase in the active power consumption of the VCO.

The above analysis indicates that the aSAT solver generates a limited number of keys within a small range of the target frequency and voltage amplitude. The remaining keys result in frequencies and voltages that are above and below the required targets.

VI. Conclusions

A novel security oriented analog design methodology is described. A mesh based obfuscation technique is proposed that utilizes the obfuscation of the sizes of transistors to mask the biasing conditions and electrical characteristics of an analog circuit. To demonstrate the effectiveness of the technique, varactors of an LC tank based VCO are obfuscated with a 24-bit key, where each varactor is replaced by a 2x6 mesh array of transistors. The implementation of the obfuscation technique results in a 145% increase in the active area and 14% increase in the power consumption. For an area constrained analog circuit, the obfuscation technique is implemented on the sub-blocks of the analog circuit that are more limited in area. The probability to determine the correct key through brute force attack is 5.96×10^{-8}.

In addition, an SMT based aSAT algorithm is proposed to reduce the design time of implementing the parameter based obfuscation technique. The aSAT algorithm is applied to the 2x6 mesh used to obfuscate an LC tank VCO. The algorithm automatically determines obfuscated transistor sizes such that only a limited number of keys produce the correct operating conditions. The dimensions of the obfuscated transistors determined by the aSAT algorithm result in at least a 15%, 3%, 13%, and 2 dB deviation in, respectively, the effective transistor size, target frequency, amplitude, and phase noise when an incorrect key is applied. In addition, the aSAT determined transistor sizes produce only a single key that results in a target frequency of 3.25 GHz and target amplitude of 1.66 V. Although other keys produce frequencies close to the target frequency, the output voltage of the VCO deviates significantly from the target value, resulting in at least a 2 dB degradation in the phase noise of the VCO. The proposed mesh technique with SMT-based optimization, therefore, provides a novel approach to securing an analog circuit from IC theft, reverse engineering, and counterfeiting.

Acknowledgments

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

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] J. Wang, C. Shi, A. Sanabria-Borbon, E. Snchez-Sinencio, and J. Hu, "Thwarting Analog IC Piracy Via Combinational Locking," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 1–10, October 2017.

[3] R. Torrance and D. James, "The State-of-the-Art in Semiconductor Reverse Engineering," *Proceedings of the IEEE/ACM Design Automation Conference*, pp. 333–338, June 2011.

[4] R. Torrance and D. James, "The State-of-the-Art in IC Reverse Engineering," *Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 363–381. September 2009.

[5] M. Zabeli, N. Caka, M. Limani, and Q. Kabashi, "The Impact of MOSFET's Physical Parameters on Its Threshold Voltage," *Proceedings of the 6th Conference on Microelectronics, Nanoelectronics, Optoelectronics*, pp. 54–58, May 2007.

[6] J.M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*, 2008.

[7] K.E. Kroell and G.K. Ackermann, "Threshold Voltage of Narrow Channel Field Effect Transistors," *Journal of Solid-State Electronics*, Vol. 19, No. 1, pp. 77–81, January 1976.

[8] IBS Corporation, "IBS Corporation, Industry Reports," 2003.

[9] 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.

[10] R. Mukul, A. Biere, and A. Gupta, "A Survey of Recent Advances in SAT-Based Formal Verification," Vol. 7, No. 2, pp. 156–173, April 2005.

[11] 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.

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

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

[14] V. V. Rao and I. Savidis, "Transistor Sizing for Parameter Obfuscation of Analog Circuits Using Satisfiability Modulo Theory," *Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 102–106, October 2018.