Protecting Analog Circuits with Parameter Biasing Obfuscation

Vaibhav Venugopal Rao and Ioannis Savidis
Department of Electrical and Computer Engineering
Drexel University, Philadelphia, PA 19104
vv85@drexel.edu, isavidis@coe.drexel.edu

***Abstract*—A methodology to secure analog intellectual property (IP) by obfuscating biasing conditions is presented in this paper. Previous research methodologies have focused on protecting digital IP from theft, overproduction, counterfeiting, and Trojan insertion. Analog IP has not been investigated as it does not share the same replicated structures and functionalities used for digital protection. The bias encryption techniques presented in this paper are implemented on a phase locked loop (PLL). The operating frequency of the PLL is masked in the range of 800 MHz to 2.2 GHz with a 40-bit encryption key. The probability of determining the correct key through brute force attack is 9.095×10^{-13}. The overheads of encrypting the PLL include a 6.3% increase in active area, a 0.89% increase in power consumption, and a 5 dBc/Hz increase in phase noise.**

I. Introduction

Integrated circuits (ICs) are an essential part of any electronic device. ICs are broadly used in products ranging from household devices to defense systems. Modern integrated circuits often include digital, analog, and radio frequency components on a single die [1]. Over the last few decades, a rapid growth in the IC market has lead to the globalization of the IC supply chain. As a result of globalization, manufacturing has shifted from trusted in-house to untrusted offshore foundries. While offshore production has resulted in the reduction of the cost of an IC, concerns in reliability and security have increased. An untrusted third-party foundry is capable of intellectual property (IP) theft, IC counterfeiting, IC overproduction, and the insertion of malicious circuitry (hardware Trojans), which poses an important new security threat to systems that rely upon these untrusted ICs.

With the global semiconductor industry estimated to have generated revenues of $345 billion dollars in 2013, approximately $54 billion was contributed by the analog IC market [2]. Although a large number of modern electronic components are digital, most function in a world of continuously varying analog inputs. The analog circuits are small as compared to the digital components, however, due to increased complexity, a large amount of time and resources are allocated for analog IC design. Electronic products from appliances and cell phones in consumer electronics to radars and communication devices used in military applications often include analog circuits that are integrated with digital computing cores.

Techniques to protect analog intellectual property are mostly overlooked as analog ICs typically have a small footprint and are challenging to design. Analog IC design significantly differs from digital design, and includes:

1) greater precision in biasing conditions,
2) greater sensitivity to noise and temperature,
3) greater emphasis on signal integrity,
4) tighter noise margins,
5) simultaneous consideration of multiple parameters of the design process (whereas digital circuits follow a sequential design flow), as shown in Fig.1.

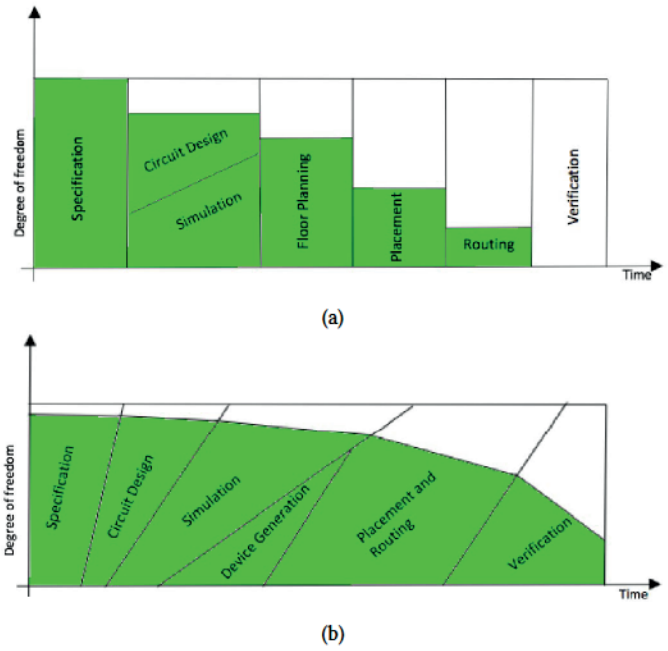

Fig. 1: Comparison of design flows. a) Stepwise reduction of degrees of freedom for digital circuits, and b) continuous reduction of degrees of freedom and overlap of design flow for analog circuits [3].

The additional design considerations for analog ICs results in increased challenges when implementing security features. In addition, the complexity of the design motivates an adversary to steal or counterfeit analog IP to save time and resources. There are a limited number of techniques for analog IP protection, with watermarking [4, 5] and camouflaging [6, 7] predominantly used. Although both techniques protect analog circuits, the end user or foundry are not prevented from reverse engineering and counterfeiting the

978-1-5386-0415-1/17/$31.00 ©2017 IEEE

IP, as the foundry has access to all information pertaining to the production of the IC.

The primary contribution of the work described in this paper is the development of an obfuscation technique to protect analog IP from counterfeiting and IC overproduction. A technique that obfuscates the critical biasing conditions of an analog circuit is developed, masking the desired functional parameters of the circuit block. The proposed technique is implemented on a phase locked loop local oscillator to mask the target mixer frequency of a superheterodyne receiver.

A discussion on the assumed threat model is provided in Section II. The circuit model and critical parameters of an analog phase locked loop (PLL) are described in Section III. A brief discussion on analog obfuscation is provided in Section IV. An overview of logic encryption is described in Section V, followed by an explanation of the proposed analog obfuscation technique in Section VI. An implementation of the proposed technique on a phase locked loop (PLL) and results characterizing the obfuscated circuit are described in Section VII. Concluding remarks are offered in Section VIII.

II. Threat Model

An untrusted foundry model is assumed, where the foundry has access to the IC design and possesses the necessary tools and skills to counterfeit and overproduce the circuit from the provided GDS-II file [8]. In addition, the circuit in the design stage is assumed trusted and devoid of any malicious components.

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 IP with feature sizes smaller than 50 nanometers [9].

III. Characteristics of Analog Phase Locked Loops

Accurate characterization of device parasitics and process, voltage, and temperature (PVT) variations are necessary to guarantee the correct performance of an analog IC. Parameter characterization is critical in setting the proper biasing conditions of the analog circuit, which directly affects the circuit performance. In this section, an overview of the phase locked loop (PLL) and a description of critical PLL parameters are provided.

A. Phase Locked Loops

Phase locked loops (PLLs) are an essential part of an integrated circuit. The primary task of the PLL is to provide a cyclic output signal that maintains phase coherence with a reference input signal. A low frequency reference clock is used as an input, which is typically provided by an off-chip crystal oscillator, and is multiplied by a ratio N to generate a high frequency clock. The PLL is used as a high frequency clock, a frequency multiplier, or for clock de-skew. The five main components of a PLL are the phase-frequency detector (PFD), charge-pump (CP), loop filter (LF), voltage controlled oscillator (VCO), and frequency divider, as shown in Fig. 2.

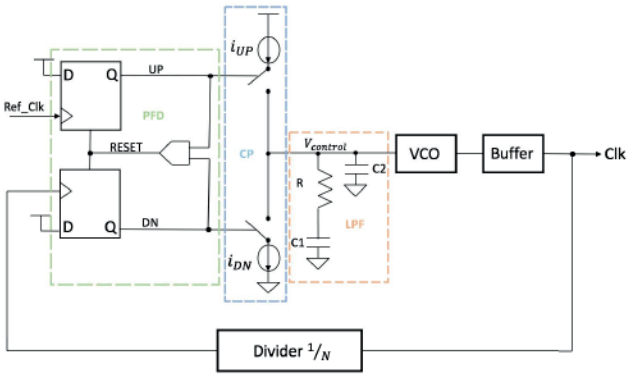

Fig. 2: Block diagram of a Type-II 3rd order PLL [10].

1) Phase-Frequency Detector: The phase-frequency detector (PFD) generates a voltage signal corresponding to the phase difference between the reference clock and feedback path. When the phase difference of the two input signals to the PFD is zero, the PFD generates a constant output voltage. In this paper, the PFD is implemented using a positive edge triggered D flip-flop (DFF) topology. The benefits of using the DFF based PFD are: 1) there is no dependency on the duty cycle of the input, 2) the PFD exhibits a $\pm 180°$ static phase shift, and 3) a constant gain over a range of 2π phase difference is provided. The D flip-flop based PFD produces two outputs, UP and DOWN, depending on the phase difference between the reference and feedback signals.

2) Voltage Controlled Oscillator: The voltage controlled oscillator (VCO) generates an oscillation frequency controlled by an input voltage from the charge pump. The performance of the PLL has significant dependence on the design of the VCO. A schematic of an LC VCO is shown in Fig. 3.

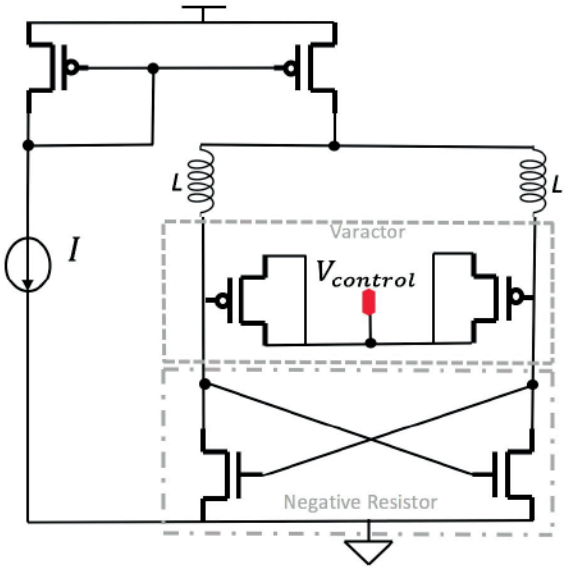

Fig. 3: Circuit diagram of a LC VCO.

The oscillation frequency of the LC VCO is

$$F_{LC} = \frac{1}{2\pi\sqrt{LC}}\,, \tag{1}$$

where F_{LC} is the center frequency of the LC oscillator, L is the inductance, and C is the capacitance. The VCO includes a varactor capacitance in addition to the parasitic capacitances of the circuit.

3) Frequency Divider: The divider generates an output signal whose frequency is a fraction of the frequency generated by the VCO. Frequency dividers are implemented in a PLL to permit a phase comparison of the output signal from the VCO with the input reference signal from the off-chip crystal oscillator by the phase-frequency detector.

A linear model of the PLL is shown in Fig. 4, which is used to determine the transfer function and phase noise. The transfer function of a typical PLL derived from the linear model is given by (2), where ϕ_{out} represents the output phase, ϕ_{in} is the phase of the input signal, K_{CP} is the gain of the charge pump, H_{LF} is the gain of the low pass filter, K_{VCO} represents the gain of the VCO, and N denotes the order of the PLL [11]. The general form of the transfer function of the PLL is $H(S) = \frac{\omega_c}{s+\omega_c}$, which corresponds to the transfer function of a low pass filter. The PLL therefore behaves like a low pass filter of the input reference signal [10].

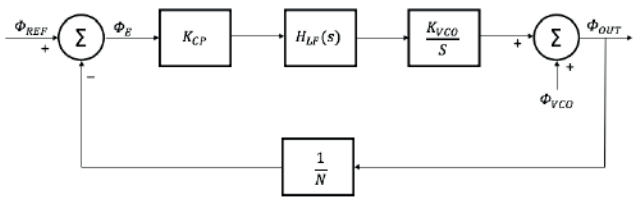

Fig. 4: Linear model of a PLL [10].

$$\frac{\phi_{out}}{\phi_{in}} = \frac{K_{CP}H_{LF}(S)K_{VCO}N}{sN + K_{CP}H_LF(s)K_{VCO}} \tag{2}$$

B. Phase Noise

Phase noise is the frequency domain representation of random fluctuations in the signal waveform. Jitter is the time domain representation of phase noise. For an ideal oscillator, the frequency domain representation of the output frequency is a pair of Dirac delta functions. Due to phase noise, the power of the signal is spread to adjacent frequencies. The phase noise includes low frequency flicker and white noise and is expressed in units of dBc/Hz. For a PLL, the phase noise is typically measured at frequencies of 1 kHz and 1 MHz. The phase noise of the VCO in the frequency and time domain is given by, respectively,

$$\frac{\phi_{out}}{\phi_{VCO}} = \frac{sN}{sN + K_{CP}H_LF(s)K_{VCO}}\,, \tag{3}$$

and

$$Jitter_{sec} = \frac{\sqrt{\int_{-\infty}^{\infty} 10^{\frac{PhaseNoise_{dBc/Hz}}{10}}}}{2\pi f}\,, \tag{4}$$

where f is the center frequency of the PLL, K_{CP} is the gain of the charge pump, K_{VCO} is the VCO gain, and $H_{LF}(s)$ is the transfer function of the filter stage [12]. The general form of (3) is $H(S) = \frac{s}{s+\omega_c}$, which is the transfer function of a high pass filter. The PLL therefore behaves like a high pass filter for the output signal produced by the VCO. In addition, when s approaches zero, the phase noise with respect to the reference clock signal increases linearly with the divider ratio N.

C. Settling Time

The settling time is the amount of time required to return to the ideal operating conditions of the PLL on the application of a step input, which characterizes the response and recovery of the PLL to noise or erroneous inputs. The propagation delay of the circuit and the time required for the output to settle to within the specified error are included in the settling time. For a PLL, the settling time is the duration required for the output to settle to a particular frequency in response to phase shifts in the circuit. The settling time is frequently measured in terms of the damping factor ζ given by [13, 14]

$$\zeta = \frac{1}{2}\sqrt{\frac{\omega_1}{K_v}}\,, \tag{5}$$

where K_v is the product of the phase detector gain and the gain of the VCO and ω_1 is the 3 dB cutoff frequency of the VCO.

IV. Analog Obfuscation

The obfuscation of digital circuits entails the masking of boolean functions and logical values [15, 16]. Analog circuit operation, however, depends on a continuous range of input/output values as well as the setting of various biasing parameters, resulting in increased complexity when implementing obfuscation of analog blocks. In addition, analog circuits are tightly designed within parameter bounds to match target gains, phase noise, and bandwidth, with any added circuitry causing shifts in the parameter characteristics. The challenge therefore becomes obfuscating the circuit while minimally affecting circuit parameters.

The proposed technique targets obfuscation of critical circuit parameters of the analog block, including the gain of an amplifier, cutoff frequency of filters, and the operating frequency of a PLL. As analog circuits are typically designed in stages, distributing the key bits across critical circuit parameters of each stage results in low area overhead and reduced impact on the circuit parameters.

V. Key Based Parameter Obfuscation

Analog ICs are significantly more sensitive to noise and temperature (tighter noise margins) as compared to digital circuits. Setting the correct biasing points in an analog circuit is therefore critical to establish the proper operating conditions, as circuit functionality and performance are directly dependent on the set bias voltages and currents. The proposed key based obfuscation technique 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 set at the target node. The technique is applicable to various biasing parameters including setting the voltage/current at a node or modifying the gain of the circuit.

A. Obfuscation of Voltage Biasing Node

A typical voltage biasing circuit is shown in Fig. 5(a). The obfuscated biasing circuit produces resistances R_1 and R_2 that are directly proportional to the combined width of the active transistors, as shown in Fig. 5(b). Only on application of the correct key sequences KEY1 and KEY2 are the proper transistor widths selected and therefore, the proper resistances set, resulting in the desired V_{out}.

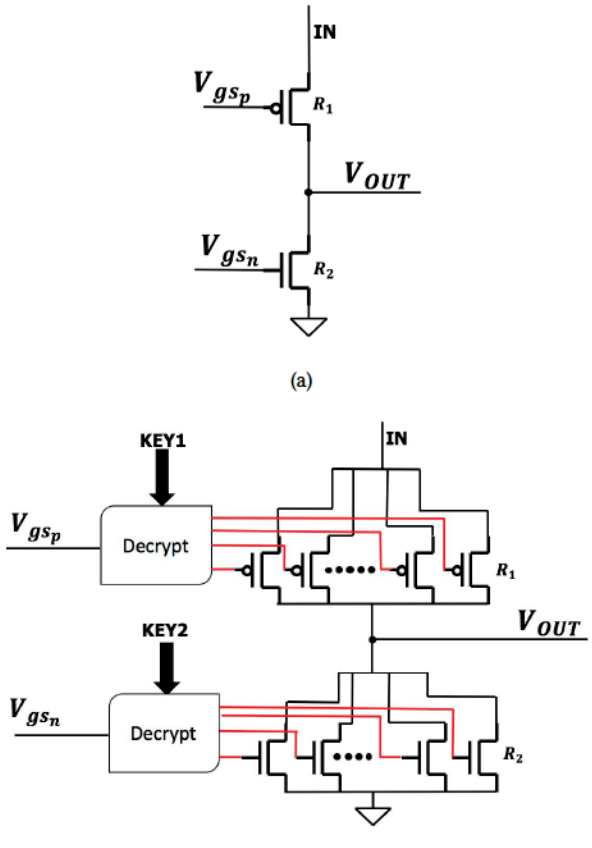

Fig. 5: Voltage bias circuit that is a) unencrypted and b) obfuscated.

B. Obfuscation of Current Biasing Node

The current at a target node is given by (6), which is the drain to source current I_{ds} of a transistor operating in the linear mode. The output current I_{ds} is directly proportional to the width of the transistor.

$$I_{ds} = \mu_n C_{ox} \frac{W}{L}[(V_{gs} - V_t)V_{ds} - \frac{V_{ds}^2}{2}] \quad (6)$$

A typical current bias circuit is shown in Fig. 6(a). The secured current bias circuit implemented with the proposed technique is shown in Fig. 6(b). When the correct key sequence KEY1 is applied, the appropriate transistor widths are set, establishing the desired current bias I_{ds}.

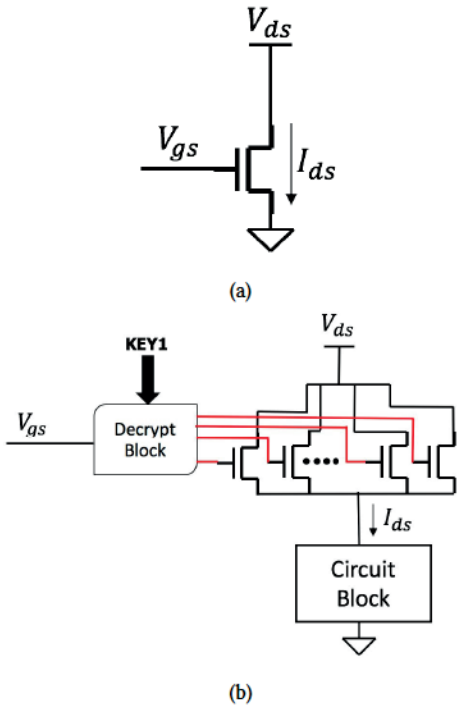

Fig. 6: Current bias circuit that is a) unencrypted and b) obfuscated.

The proposed technique is applicable to the obfuscation of other width dependent circuit parameters including capacitance and gain.

VI. Implementation Of Key Based Width Obfuscation on a PLL

In the analog domain, an emphasis on research and product development has focused on radio-frequency front-end circuits. A typical RF superheterodyne receiver consists of a combination of amplifiers, a mixer, a filter, a PLL, and a demodulator, as shown in Fig. 7. The objective is to obfuscate each stage of the superheterodyne receiver using the proposed width based obfuscation technique. A 512-bit key secures the parameters of the receiver, with 40-bits used for the obfuscation of the PLL frequency. The performance of the obfuscated PLL is compared with a standard PLL.

The proposed width based parameter obfuscation technique is implemented on a type-II 3rd order phase locked loop (PLL) for the mixer block of a superheterodyne receiver. The type-II 3rd order PLL provides greater flexibility to adjust the loop bandwidth and gain. In addition, a type-II PLL offers a wider acquisition range and is ideal for high-performance digital integrated circuits [11]. As shown in Fig. 2, the five main components of a type-II 3rd order PLL are the phase-frequency detector (PFD), the charge-pump (CP), the loop

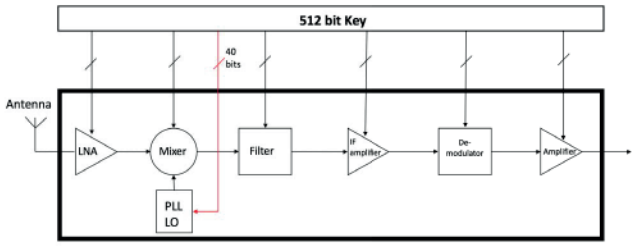

Fig. 7: Block diagram of a superheterodyne receiver with an integrated PLL local oscillator (LO).

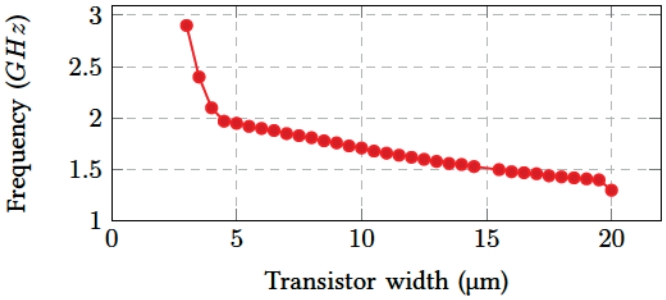

Fig. 8: Characterization of the VCO frequency as a function of the width of the negative resistor.

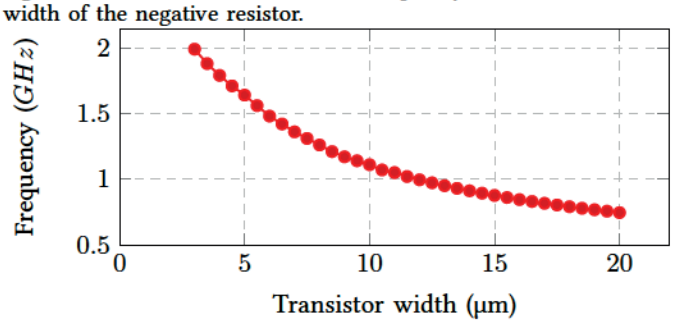

Fig. 9: Characterization of the VCO frequency as a function of the width of the varactor.

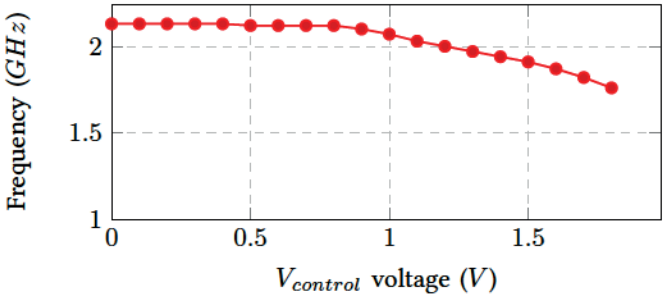

Fig. 10: Characterization of the VCO frequency as a function of the control voltage.

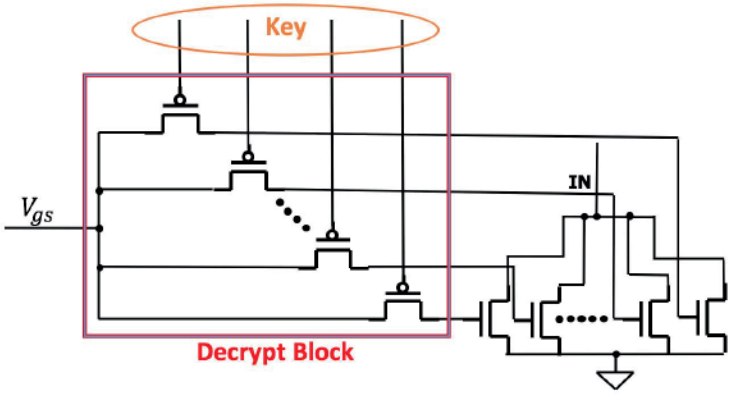

Fig. 11: Schematic of the decryption block.

filter (LF), the voltage controlled oscillator (VCO), and the frequency divider.

The PFD is based on an edge triggered D flip-flop architecture as described in Section III. The charge pump is a cascode design to minimize charge sharing and to suppress voltage spurs. The selection of an LC based VCO provides superior phase noise performance as compared to other VCO topologies [11]. A divide by 32 frequency divider is implemented to permit comparison of the phase of the input signal from the off-chip crystal oscillator with the phase of the output signal from the PLL.

The biasing parameters of the VCO selected for obfuscation are: 1) the range of the control voltage, 2) the size of the varactor, and 3) the size of the negative resistance circuit. The three chosen biasing parameters significantly impact the frequency range, lock-in range, bandwidth, and jitter performance of the PLL. The variation in the output frequency of the VCO due to the negative resistance circuit, varactor, and control voltage is shown, respectively, in Figs. 8, 9, and 10. The dependence of the output frequency on the sizes of the transistors in the VCO is used to implement the proposed security technique and mask the true output frequency of the PLL.

The varactor and negative resistance circuit are divided into 10 transistor widths on both symmetric current paths of the VCO. A total of 40 transistors are therefore implemented to mask the VCO output frequency. Only when the correct key sequence is applied will the VCO produce the expected output frequency. The key sequences are distributed by means of a simple pass transistor topology, as shown in Fig. 11.

VII. Results

The un-obfuscated and obfuscated PLLs are designed in a 180 nm CMOS process. An input reference clock of 55 MHz was used, and the target operating frequency of the PLL was 1.75 GHz.

The active transistor area of the PLL increased by 6.3% from 6.885 μm^2 to 7.319 μm^2 when accounting for the additional transistors and the key-delivery circuit. The key length for the obfuscated circuit is 40 bits. The probability of obtaining the correct frequency of the PLL under ideal conditions through brute force attack is 9.095×10^{-13}. The probability is further reduced by adding additional key bits with the corresponding parallel transistor widths. Although an incorrect key produces an output from the PLL, the

frequency will not match the 1.75 GHz target, requiring an adversary to observe all input-output combinations to correctly determine the key. The comparison of the critical parameters of an obfuscated and un-obfuscated PLL are listed in Table I.

TABLE I: Characterization of obfuscated and unobfuscated PLLs.

Parameter	Unobfuscated PLL	Obfuscated PLL
Locking Frequency	1.75 GHz	1.76 GHz
Area	6.885 μm^2	7.3192 μm^2
Settling Time	300 ns	700 ns
Power	22.1 mW	22.3 mW
Phase noise @1MHz	-116.5 dBc/Hz	-111.1 dBc/Hz
Phase noise @1kHz	-30.59 dBc/Hz	-26.51 dBc/Hz

VIII. Design Insight for Implementing Parameter Obfuscation

A challenge faced during the design and characterization of the obfuscated PLL was the high sensitivity of the circuit to variations in device parameters and parasitics. Any deviation of device parameters resulted in a penalty in performance. The additional transistors needed to implement the obfuscation technique resulted in increased parasitics, which required further circuit optimization to meet the target performance.

The inter-dependence of biasing conditions caused additional challenges, in particular when trying to determine transistor widths that produce a limited set of unique keys. There were redundant biasing conditions that produced the desired output frequency, and eliminating these conditions was a challenge.

Although process, voltage, and temperature (PVT) variations typically produce undesired effects on circuit parameters, there are potential benefits when used to generate an unique key sequence for analog circuit blocks. Analog circuits in sub-90nm technology nodes are particularly vulnerable to process variations [17]. Post silicon tuning of analog circuits compensates for PVT based variations, where an offset voltage is determined and applied to the circuit to counteract the effects. PVT compensation complimented with the proposed width obfuscation technique results in a two stage protection, where an initial key is required to coarsely set the biasing conditions of the circuit and a second key is used to fine tune the targeted parameters. An additional benefit is that each analog IC now requires a unique key, as the tuning of parameters differs between dies.

IX. Conclusions

A unique analog obfuscation technique that implements key-based logic encryption is described. A VCO based reference PLL and obfuscated PLL were implemented in a standard 180 nm CMOS process to demonstrate the implementation of the proposed technique. Circuit parameters including the settling time, power, and phase noise for both the obfuscated and un-obfuscated PLL were characterized. An improvement in the security of an analog IC is achieved when implementing the proposed technique with a 6.3% increase in area, 0.89% increase in power consumption, and 5 dBc/Hz increase in phase noise. The probability of determining the correct key sequence through a brute force attack is $9.095x10^{-13}$. By implementing the proposed technique on multiple analog components in the integrated circuit, the key space is increased and the overall security is further improved. The analog obfuscation technique complements existing digital logic encryption to further protect modern ICs. The proposed technique is therefore an effective countermeasure against IP theft, counterfeiting, and overproduction of analog and mixed signal circuits.

References

[1] ITRS, "International Technology Roadmap for Semiconductors," March 2011.

[2] Semiconductor Industry Association, "The U.S. Semiconductor Industry: 2014 FACTBOOK," March 2014.

[3] J. Scheible and J. Lienig, "Automation of Analog IC Layout: Challenges and Solutions," *Proceedings of the ACM International Symposium on Physical Design (ISPD)*, pp. 33–40, March 2015.

[4] J. D. Carothers J. J. Rodriguez W. T. Holman. R. D. Newbould and, D. L. Irby, "Mixed Signal Design Watermarking for IP Protection," *Proceedings of the Southwest Symposium on Mixed-Signal Design*, pp. 249–265, January 2003.

[5] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "IP Protection for VLSI Designs Via Watermarking of Routes," *Proceedings of the IEEE International ASIC/SOC Conference*, pp. 406–410, September 2001.

[6] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging," *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*, pp. 709–720, November 2013.

[7] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1207–1228, August 2014.

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

[9] 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.

[10] M. T. Hsieh and G. E. Sobelman, "Comparison of LC and Ring VCOs for PLLs in a 90 nm Digital CMOS Process," *Proceedings of International SoC Design Conference ((ISOCC)*, pp. 19–22, October 2006.

[11] B. Razavi, *Design of Integrated Circuits for Optical Communications*, McGraw-Hill, Inc., 2003.

[12] A. Hajimiri, "Noise in Phase-Locked Loops," *Proceedings of the IEEE Southwest Symposium on Mixed-Signal Design*, pp. 1–6, February 2001.

[13] B. Razavi, *Design of Analog CMOS Integrated Circuits*, McGraw-Hill, first edition, 2001.

[14] T. H. Lee, *The Design of CMOS Radio-Frequency Integrated Circuits*, Cambridge university press, 2003.

[15] K. Juretus and I. Savidis, "Reducing Logic Encryption Overhead Through Gate Level Key Insertion," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1714–1717, May 2016.

[16] K. Juretus and I. Savidis, "Reduced Overhead Gate Level Logic Encryption," *Proceedings of the IEEE/ACM Great Lakes Symposium on Very Large Scale Integration (GLSVLSI)*, pp. 15–20, May 2016.

[17] M. White and Y. Chen, "Scaled CMOS Technology Reliability Users Guide," *Report on Electronic Parts and Packaging (NEPP) Program Office of Safety and Mission Assurance, Jet Propulsion Laboratory, National Aeronautics and Space Administration*, pp. 1–22, March 2008.