How Multi-threshold Designs Can Protect Analog IPs

Abdullah Ash- Saki
Dept. of Electrical Engineering
Pennsylvania State University
University Park, USA
axs1251@psu.edu

Swaroop Ghosh
Dept. of Electrical Engineering
Pennsylvania State University
University Park, USA
szg212@psu.edu

***Abstract*— Analog Integrated Circuits (ICs) are one of the top targets for counterfeiting. However, the security of analog Intellectual Property (IP) is not well investigated as its digital counterpart. In this paper, we explore the possibility of multi-threshold voltage (V_{TH}) design to protect the analog IP from Reverse Engineering (RE)-based attacks. Analog circuits are sensitive to V_{TH} as the operating region of a transistor can vary with V_{TH}. Furthermore, the V_{TH} of individual transistors cannot be identified during the RE process. The trial-and-error based technique to guess the V_{TH} and validate with a golden IC will ramp up RE effort exponentially. Thus, by carefully including multi-V_{TH} transistors, the designer can ensure that the properties of analog IP e.g., gain, bandwidth, and linearity are protected even though the physical dimensions of the transistors are revealed. We demonstrate this technique by using a case study on a wide-swing cascode amplifier. Simulations show that incorrect V_{TH} inference can lead to substantially degraded performance like 98 dB drop in open-loop gain and up to 19% increase in total harmonic distortion. Based on V_{TH} choice, the proposed technique can save ~ 3% area over conventional design. We show that the reverse engineering effort can be ~10^{13} years. We propose a technique like transistor splitting to increase the effort even more. Mismatch analysis shows that the proposed technique results in only 1% loss in mean robustness.**

Keywords—analog hardware security, reverse engineering, multi-threshold voltage design.

I. INTRODUCTION

Semiconductor supply chain is increasingly getting exposed to a variety of vulnerabilities such as Trojan insertion, cloning, counterfeiting, over-production, recycling, Reverse Engineering (RE) etc. [1]. The annual loss due to Intellectual Property (IP) breach is about $4 billion [2]. These security vulnerabilities are being addressed by different schemes e.g., hardware metering [3-4], remote IC activation [5], Physically Unclonable Function (PUF) [6], reconfigurable logic barrier [7], secure split test [8], Ending Piracy of Integrated Circuits (EPIC) [9] and so on. Majority of the efforts in hardware security domain has been confined to digital circuits. However, existing research lacks treatment of the security of Analog and Mixed-Signal (AMS) and Radio Frequency (RF) circuits. One possible reason could be the disparity between the number of transistors in digital design and analog design. Less number of transistors in analog design makes it vulnerable to attacks like RE. AMS designs e.g., amplifiers, Analog-to-Digital Converter (ADC), Digital-to-Analog Converter (DAC), filter and voltage regulators, and, RF ICs are part of nearly all computing systems with applications ranging from healthcare, mobile, internet-of-things to supercomputers. According to IHS technology, analog IP is the most counterfeited among all semiconductor products [10].

Even though the threats on analog design are identical to their digital counterparts, the modes of attacks are very different. The IP protection mechanisms for digital systems e.g., logic encryption and camouflaging cannot be directly extended to analog systems. The negative impact of extra parasitic from protective countermeasures (e.g., Extra transistors to obfuscate the design) make the security of analog design further challenging. In this paper, we propose a method to prevent RE-based attacks.

Background on RE: In RE, the adversary de-packages the Integrated Circuit (IC), delayers the IC, and takes pictures of each layer [11]. The images of metal layers provide connectivity information whereas the image of the base layer is employed to identify the transistor setup. Finally, the information obtained from the images are stitched together to prepare a netlist unlocking the IP.

Previous works on analog hardware security: Previous works on analog hardware security is relatively scarce. In [12] split manufacturing is proposed to protect RF circuits from the untrusted foundry. In [13], a secure sense amplifier is proposed which uses a memristor-based voltage divider to bias body voltage of transistors in the amplifier to ultimately protect against evil-maid attack. The arrangement is such that the memristance is tuned based on a user input key. If the user provides an incorrect key, the memristor cross-bar based programming circuit will generate a high programming voltage (V_{PROG}) that will cause memristor breakdown in the voltage divider. Therefore, the voltage divider will generate a high body bias voltage which will result in an unreasonably high offset in the sense amplifier, and thus, will permanently disable the chip. While the proposition conceptually seems promising, it faces certain challenges. *First*, to cause a breakdown, the programming circuit should have a high supply voltage ≥ 6.4V ($2 \times V_{Breakdown}$, 3.2V as mentioned in the paper). At such high supply voltages, memristors in the crossbar array of the programming circuit will experience resistance drift. Therefore, during run-time, even with correct-key, the programming circuit can generate incorrect programming voltage. *Second*, the scheme does not provide sufficient protection against RE attacks as the memristor-based adaptive body-bias arrangement is not a mandatory part of the chip. After delayering and imaging, the adversary can: (i) adopt a different offset compensation scheme or, (ii) implement his own memristor programming circuit to ensure $V_{PROG} < V_{Breakdown}$ which is fairly simple (one easy way is to scale down the supply of the programming circuit so that

This work is supported by Semiconductor Research Corp. (2018-TS-2847), NSF (CNS-1722557, CNS-1814710, CCF-1718474, DGE-1723687, and DGE-1821766) and DARPA Young Faculty Award (D15AP00089).

2576-6996/18/$31.00 ©2018 IEEE
DOI 10.1109/ICCD.2018.00075

V_{PROG} never exceeds break-down voltage). In [14], key-based obfuscation of biasing voltage and the current node is proposed. The idea is to have multiple parallel transistors in the biasing circuit and based on a correct key, a specific number of those transistors will be activated so that an expected (W/L) is achieved. However, [14] has limitations as there could be multiple correct keys, and performance degradation from an incorrect key is not significant [15]. The work in [15] proposes a similar but supposedly better key-based obfuscation addressing these issues. In [15], the authors propose a configurable current mirror that can only be configured with a correct key. The current mirror has a grid of switches (transistors) that connects to parallel current branches each with different size $\alpha_i(W/L)$. Satisfiability Modulo Theorem is then applied to determine the α_i values. Based on a correct key, correct numbers of parallel branches are activated giving out correct $\sum\alpha_i(W/L)$ and correct I_{OUT}.

Although the combinational locking techniques in [14] and [15] can effectively protect against IC recycling and thwart inauthentic users, both are vulnerable against RE based IP infringement. An adversary can try to break the security by following: From delayering and imaging, the adversary will know the minimum W/L, $(W/L)_{min}$ and maximum W/L, $(W/L)_{max}$ (which is the summation of W/L ratios of all parallel branches). Then, the adversary can sweep (W/L) from $(W/L)_{min}$ to $(W/L)_{max}$ and note the $(W/L)_{target}$ that matches the target specification and/or gives the highest performance. The (W/L) sweep will take substantially less time than checking 2^N combinations (N = bits size of the key).

Proposed idea: In this work, we propose a multi-threshold voltage (V_{TH}) based secure analog design to protect against RE based attack. Multi V_{TH} transistors are used in modern process technologies to make trade-offs between leakage and performance. Low V_{TH} (LVT) transistors are used to improve the performance at the cost of leakage whereas high V_{TH} (HVT) is used to improve leakage at the cost of performance. In analog designs, multi-V_{TH} transistors are commonly used [16]-[19] to deal with different constraints. For example, in low-power analog designs, low-V_{TH} transistors are used to overcome the headroom issue. However, in this paper, the application space of multi-V_{TH} transistors is extended beyond enabling low-power operation. The idea is to replace few Normal V_{TH} (NVT) transistors from an existing analog design with LVT and/or HVT transistors while keeping the original performance metrics e.g., gain, bandwidth, total harmonic distortion etc. If the adversary fails to guess the V_{TH} of the transistors correctly then he or she will obtain unusable analog performance and thus, protecting the IP from RE based attacks. For example, the common source amplifier in Fig. 1(a) shows visible difference between no-load gains (Fig. 1(b)) of a correct V_{TH} design and an incorrect V_{TH} design (in transistor M2; correct V_{TH} = 273 mV, incorrect V_{TH} = 423 mV). This example clearly indicates that the analog designs will be protected if an adversary fails to identify the V_{TH} correctly. Since the identification of transistor V_{TH} requires sophisticated equipment and is costly (see, Section II C), we assume that the adversary will rely on a guess-and-validate approach which will be time intensive and can be made impractical. Moreover, the proposed technique can be used in conjunction with the key based combinational locking technique from [15]. Although multi V_{TH} transistors find its application in digital hardware security [20]-[22], its application in analog *security* domain is not explored. In this paper, for the *first time, we report secure analog design using multi V_{TH} transistors.*

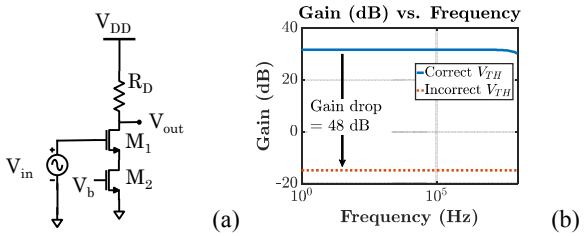


Fig. 1. (a) A common-source amplifier and (b) no-load gains with correct and incorrect V_{TH} of M_2 transistor.

To this end, we make the following contributions in this paper. We,

- Propose a secure analog design philosophy with multi-threshold transistors that can thwart RE efforts.
- Present applicability of the proposed idea with a design example of an operational amplifier and G_m-C filter.
- Run process variation analysis to compare robustness with traditional designs and report associated overheads.
- Evaluate the RE effort and suggest techniques to improve the RE effort.

Rest of the paper is organized as follows: in Section II we discuss the scope of our work and possible attack models. In Section III, we present different components of the secure multi-threshold design with an example of an op-amp with biasing circuits. In Section IV, we present combined design along with overhead, variation, and RE effort analysis. General guidelines for multi V_{TH} based secure design that can be extended to other class of analog designs are also discussed with an example of secure G_m – C low pass filter. Finally, we draw conclusion in Section V.

II. Attack Model And Scope Of The Work

A. Overview

Any kind of analog design depends on correct voltage and current biasing and correct operating regions of the transistors. We can ensure correct bias levels and operating regions in two ways, (a) NVT transistors with nominal sizing; and, (b) LVT or HVT or a mixture of HVT/LVT transistors with proportionally scaled-up/down sizing. We propose careful inclusion of properly sized LVT and/or HVT transistors in the design to make the design secure. If adversary reverse-engineers and obtains transistors sizes and connections, he can first run simulations to validate the design. However, if the adversary assumes all the transistors are NVT that will lead to improper biasing voltages and branch currents and will force some performance critical transistors out of the desired operating region. Without correct biasing and operating region, the analog circuit may perform erratically. To unmask the performance, adversary can launch attacks described in Section II C in addition to optical imaging-based RE. Each of the attacks adds up to RE effort. Transistor resizing for LVT/HVT elements may leave clues to the adversary. However, there are no reference chips with all NVT transistors with which the adversary can compare the design under attack and infer the V_{TH} value from

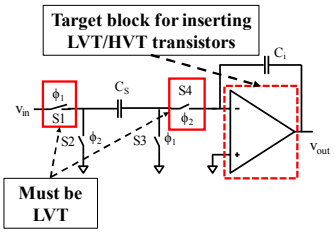
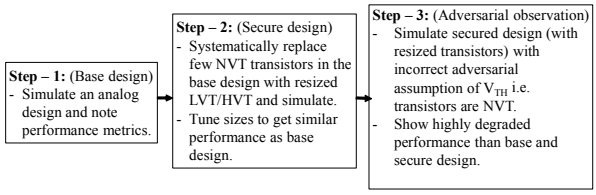


Fig. 2: Switches (transmission gates) S_1 and S_4 in the low voltage integrator in [17] must have LVT transistors to achieve full signal transmission with acceptable ON-resistance to allow low voltage operation. Therefore, the amplifier (inside the dashed-box) may be the target block for systematically inserting multi- V_{TH} transistors to secure the design from RE attacks.

the sizing. To the adversary, the V_{TH} – masked design is the reference chip. One can argue that common analog design topologies have predictable sizing and any deviation from that will make V_{TH} inference trivial. However, this is not true for custom designed ASICs where a designer can come up with novel topologies and uncommon sizing. Moreover, we propose applying V_{TH} changes in a symmetrical fashion which makes the inference even more difficult.

However, there are analog circuits where some blocks in the design must have multi–V_{TH} transistors to tackle design constraints (e.g., usage of LVT transistor in switches S_1 and S_4 in low voltage integrator [17], Fig. 2). Those *usual suspect* transistors are excluded from the proposed obfuscation technique. Instead, the proposed method targets the remaining blocks of the design (e.g., the amplifier in dashed-box in Fig. 2) which generally contains NVT transistors. The following diagram summarizes the flow of the proposed method:



B. Attacker Demography

The proposed IP protection technique is effective against common adversaries who have access to, (i) multiple copies of the chip to perform invasive RE and to use as golden chip, (ii) RE tools e.g., access to high precision optical imaging and X-ray imaging equipment, (iii) circuit simulators to run trial-and-error to validate their guess against a golden chip; (iv) absolute values of HVT, NVT and LVT from the process design kit. We assume that adversary does not have access to expensive equipment to probe I-V characteristics of the individual transistors. Note that, since all transistors are equally likely to be a potential candidate for V_{TH} alteration, individual transistor characterization can be prohibitively expensive and time intensive. We also assume that the adversary is reasonably smart and will be able to reduce the list of target transistors that can be potential candidates for V_{TH} alteration. This can be done by observing that any pair of transistors in the circuit topology would be altered together. Finally, we assume that the foundry is trusted since they will be aware of the V_{TH} of each transistor.

C. Attack Models

In the proposed design, the IP will not operate at rated performance without knowing the correct threshold voltages even if a netlist is obtained using RE. The adversary can resort to two approaches:

Brute force attack: The attacker will try all combinations of V_{TH} values (i.e., LVT, NVT, and HVT) for each transistor in the design and evaluate the circuit response for each of guess until the rated performance is obtained. There are three choices of V_{TH} for each transistor in the design. Therefore, if there are N transistors in the design the adversary will need to evaluate 3^N combinations. For smaller analog designs with smaller N, a brute force attack may figure out correct V_{TH} combination in finite time. Therefore, large analog designs (e.g., class D amplifier [23]) with more transistors are naturally more suitable for the proposed method. With each added transistor in the design, the brute force attack time ramps up exponentially. For smaller analog designs, one approach can be splitting the transistors in parallel connection to exponentially increase the number of combinations for the adversary. This will reduce the impact of each transistor on the performance metrics in case of incorrect guess by the adversary (further explained in Section IV D). In this paper, we address this type of attack.

Micro-probing attack: While the transistor V_{TH} is not directly apparent from common RE techniques like delayering and imaging the IC, there are various methods for measuring the channel doping in the literature [22]. Among these dopant profiling techniques are spreading resistance profiling, secondary ion mass spectrometry, scanning capacitance microscopy, Kelvin force probing microscopy, and electron holography [24]-[28]. However, these techniques have limitations in both spatial resolution and accuracy [29]-[32]. Even if the available techniques could provide needed resolution and accuracy, probing V_{TH} makes the RE process highly sophisticated and more resource intensive. Therefore, the economics of RE with V_{TH} probing by sophisticated technique may not be justified for small ad hoc attackers.

III. Secure Analog Components with Multi-V_{TH} Transistors

In this section, we discuss the design of individual components of a wide swing telescopic op-amp using multi-V_{TH} transistors.

A. Simulation Setup

We identify transistors suitable for V_{TH} alteration in each component. The objectives are to ensure that, (i) we have sufficiently camouflaged V_{TH}s that will make the RE time intensive and, (ii) the design is unusable even if a single V_{TH} is guessed by the adversary incorrectly.

PTM 65nm transistors [33] are used to design and analyze the circuits. Following V_{TH} values are assumed for the simulations unless otherwise stated:

TABLE I. Threshold Voltage (V_{TH0}) Values

	LVT	NVT	HVT
NMOS (mV)	273	423	573
PMOS (mV)	-215	-365	-515

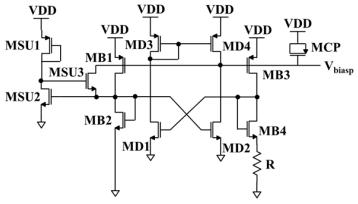


Fig. 3(a). Self-biased reference current circuit.

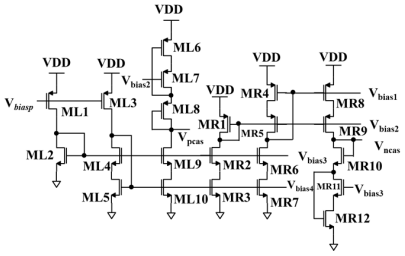


Fig. 3(b). Bias voltages generator for op-amp.

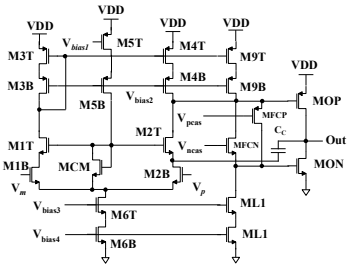


Fig. 3(c). Wide-swing telescopic cascode op-amp with output stage.

B. *Base Design*

As a study case, we have selected a wide swing telescopic op-amp with a push-pull amplifier as output stage [34] (Fig. 3 (c)). Related bias circuits (Fig. 3(a) and (b)) are also discussed. The amplifier, in normal operation, has an open loop gain of 70.6 dB and is configured to have a closed-loop gain of ~20 V/V and total harmonic distortion (THD) of ~ 0.35%. LVT/HVT transistors are incorporated to secure the design and impact the performance in case of RE. For N transistors there are 3^N possible configurations (since each transistor can be LVT, NVT or HVT) and discussing all of them is tedious and beyond the scope of this paper. Therefore, we confine our discussion to limited cases that result in a maximum loss in analog performance metrics for incorrect guess by the adversary. More results can be found in Table V.

C. *Self-Biased Reference Current Generator*

Fig. 3(a) shows a self-biased reference current generator. The reference current is given by the following equation:

$$I_{REF} = \frac{1}{8.R^2\,\mu_n\,C_{OX}\left(\frac{W}{L}\right)_2} \quad (1)$$

Where $(W/L)_2$ is the size of MB2. Among 12 transistors in the circuit (Fig. 3 (a)), four transistors (MB1-4) and the resistor (R) principally dictate the reference current and a bias voltage, V_{biasp} which is used in the next stage to generate more bias voltages for the op-amp. Each of these four transistors can have three different threshold voltages which lead to 3^4 = 81 combinations. However, to ensure symmetry and to avoid any obvious layout-level signatures, the PMOSs (MB1, 3) and NMOSs (MB2, 4) are considered as a pair and any change in threshold voltage and/or physical dimension are applied for the PMOS or the NMOS pair. This leads to 3^2 = 9 possible combinations for the reference current network. We have systematically simulated several of these combinations and reported corresponding gains, total harmonic distortions, and physical dimensions for each simulation. In majority cases, change in V_{TH} has to be counteracted by resizing transistors to ensure original performance.

Option 1 (Top PMOS pair (MB1, MB3) LVT): Resized LVT PMOS with nominal size NVT bottom NMOS pair provides higher gain (~20) and lower THD (~0.23%). If adversary makes the wrong guess about the V_{TH} then the gain drops to 0.7 and THD rises up to 19.54% and thus, deteriorates circuit performance beyond a useful margin. Fig. 4 (a)–(d) shows the transient responses and voltage transfer curves for correct and wrong V_{TH} design. Table II shows a more complete list of op-amp performance parameters. It clearly shows that the base design and the secure design has almost identical performance in terms of gain, THD, CMRR, PSRR etc. whereas for an incorrect adversarial observation, performance degrades widely. We confine our succeeding discussions to gain and THD comparison only to show the applicability of the proposed method.

Option 2 (Top PMOS pair (MB_1, MB_3) HVT): Resized HVT (W/L = 330/2) PMOS with nominal size NVT bottom NMOS pair provides higher gain (19.12) and lower total harmonic distortion (~ 0.24%). If adversary makes the wrong guess about the V_{TH} then the gain drops to 15.6 and THD rises up to 16.42%

Option 3 (Bottom NMOS pair (MB_2, MB_4) LVT): NMOS pair with this configuration has less impact. LVT NMOS gives expected performance without resizing. Thus, in case of incorrect V_{TH}, the circuit performs similarly to the nominal design as the transistor sizes remain the same.

Option 4 (Bottom NMOS pair (MB_2, MB_4) HVT): The NMOS pair is HVT and resized (MB2: W/L = 50/2 and MB4: W/L = 4×50/2) accordingly to match expected performance. However, this upsized NMOS with NVT gives almost the same gain and THD under the wrong prediction.

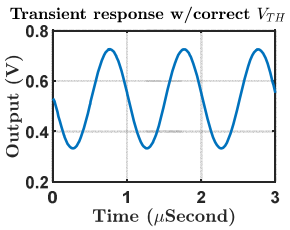


Fig. 4(a): Transient response of the amplifier with correct V_{TH}.

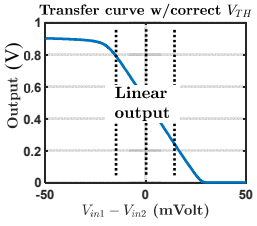


Fig. 4(b): Transfer curve of the amplifier with correct V_{TH}. Output is linear.

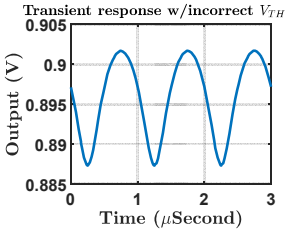


Fig. 4(c): Transient response of the amplifier with incorrect V_{TH}.

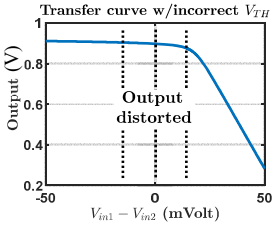


Fig. 4(d): Transfer curve of the amplifier with incorrect V_{TH}. Output clips.

TABLE II. PERFORMANCE COMPARISON CHART

Metric	Base design	Secure design	Adversarial observation
Open-loop DC gain	70.6 dB	70.6 dB	53.9 dB
THD	0.35%	0.23%	19.54%
CMRR	97.6 dB	97.7 dB	115 dB*
PSRR+ (@ 50 Hz)	50 dB	51.64 dB	43 dB
PSRR- (@ 50 Hz)	22.9 dB	22.85 dB	5.42 dB

* CMRR = 20×log (A_d/A_c). Common mode gain (A_c) drops relatively more than differential gain (A_d). Hence, the CMRR is high. However, highly degraded THD renders the op-amp unusable when reverse engineered.

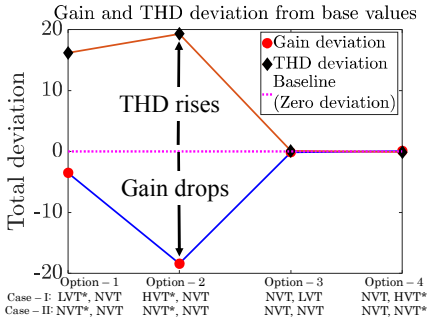


Fig. 5. Deviation from baseline specification (Case - I) for incorrect V_{TH} inference (Case – II). Some transistors have more impact than others when V_{TH} is changed. Option – 1 & 2 show large deviation from baseline and therefore are suitable for secure design. (* = Resized transistor)

Fig. 5 shows the performance comparison between two cases where case – I is the secure design with correct V_{TH} and resized (where applicable) transistors; Case – I maintains baseline performance. Case – II is when wrong adversarial assumption is made about the V_{TH}.

D. Bias Voltage Generator

This telescopic cascode op-amp topology needs five separate voltage levels ($V_{bias1\text{-}4}$ and V_{MCM}) to bias different transistors. Moreover, the push-pull amplifier in the output stage has two floating current sources (MFCP and MFCN). These transistors require two more bias voltages (V_{pcas} and V_{ncas} respectively). $V_{bias1\text{-}4}$, V_{pcas} and V_{ncas} are generated from the bias network as in Fig. 3(b). The operation of the network can briefly be described as follows: the voltage V_{biasp} from the self-biased reference current circuit is applied to mirror the current by two PMOSs ML1 and ML3. ML1 pushes a current through a relatively smaller transistor ML2 to generate a gate-to-source voltage which will be the V_{bias3} (> $2V_{DSAT}$). Similarly, ML3 pushes current through two cascode NMOSs ML4 and ML5. The gate of ML4 is biased at V_{bias3} and gate-to-source voltage of ML5 gives the V_{bias4}. The gate of ML5 is connected to the drain of ML4 to facilitate wide-swing configuration. V_{bias3} and V_{bias4} are then used to generate $V_{bias1\text{-}2}$, V_{pcas} and V_{ncas}. V_{bias3} and V_{bias4}, when applied to MR2 and MR3, pull a current from the PMOS MR1. MR1 is appropriately sized so that its gate voltage is the V_{bias2}. V_{bias2}, V_{bias3} and V_{bias4} are then applied to MR5, MR6 and MR7 respectively to generate V_{bias1}. Again, the gate of PMOS MR5 is connected with drain of MR6 for wide output swing. Finally, $V_{bias1\text{-}4}$ is used to generate V_{pcas} and V_{ncas} from gate voltages of ML8 and MR10 transistors respectively.

Option – 1 (ML3 HVT): ML1 and ML3 biased with V_{biasp} generates current that in turn determines V_{bias3} and V_{bias4}. V_{bias3} and V_{bias4} bias the tail current sources (M6T and M6B) of the op-amp. If they are too low or too high, then they can push M6T and M6B to cut-off or triode and kill the amplifier performance. To validate this theory, we replace ML3 with HVT transistor and resize that to (1000/2). With the resized HVT the branch current is almost similar and the close-loop gain and distortion are at an expected level (A_V ~ 20 and THD ~ 0.21%). However, in case of wrong threshold voltage assumption by the adversary, the wider ML3 pushes more current through ML4 and ML5. Therefore, the gate voltages (V_{bias3}, V_{bias4}) of the transistors scale-up and eventually force those in triode. The bias voltages, when applied to M6T and M6B, causes the gain drop to 0.69 and THD rise to ~ 7.96%.

Option – 2 (MR5 HVT): With correct V_{TH} the gain is 19.2 and THD is ~ 0.15%. With incorrect the $V_{TH,}$ the gain drops to 12.5 and THD increases to 7.43%. The required resized W/L is 1000/2.

E. Operational Amplifier with Output Stage

The first stage of the op-amp is a telescopic cascode and the output stage is a push-pull amplifier that gives Class – AB operation. The gain of the first stage is given by,

$$A_{V1} = g_{mN}[(r_{oN}g_{mN}r_{oN})||(r_{oP}g_{mP}r_{oP})] \quad (2)$$

And, the output stage gain without any load is given by,

$$A_{V2} = (g_{mN} + g_{mP})(r_{oP}||r_{oN}) \quad (3)$$

The op-amp under consideration has 22 transistors that lead to 3^{22} (~ 31 billion) possible combinations. We confine the discussion to several cases to validate the proposed methodology.

Option – 1 (M6T and M6B LVT): Together, these two transistors form the tail current source which controls branch currents in the op-amp and transconductance of the transistors. M6T and M6B can be made LVT with scaled-down W/L = 15/2. With this configuration the gain is ~ 20, THD is ~ 0.26% and tail current is 75 μA. However, NVT transistors with a W/L of 15/2 will give much less tail current (~13 μA) and therefore the transconductance of the transistors in the telescopic op-amp will reduce which will eventually reduce the gain. A misassumption of M6T and M6B being NVT gives a gain of 9.95×10^{-2}.

Option – 2 (M6T and M6B HVT): The op-amp can be designed with HVT M6T and M6B. However, to create a reasonable performance mismatch between HVT based secure design and corresponding NVT base adversarial observation, the transistor sizes need to be very large (W/L = 1980/2 each) which can be prohibitive in some applications like compact wearable technologies.

Option – 3 (M3T and M4T LVT): These transistors are connected to supply rail and therefore have a significant impact on the DC performance like bias current and gain. LVT M3T and M4T with a W/L of 12/2 gives a gain of ~19.2 and THD of ~ 0.15% whereas NVT M3T and M4T with same W/L (= 12/2) gives a gain of 9.96×10^{-3} and THD of 4.7883%.

Option – 4 (M3T and M4T HVT): HVT M3T and M4T with a W/L of 840/2 gives a gain of 18.9 and THD of 0.33% and the NVT assumption with same W/L gives a degraded gain of 0.33 and THD of 7.4%.

It should be noted that M3T and M4T have a significant contribution to noise. Adopting smaller LVT transistors will increase flicker noise $\left(\overline{V_n^2} = \frac{K}{C_{OX}WL}.\frac{1}{f}\right)$ and on the contrary wider HVT transistors will reduce flicker noise. This leads to a trade-off among area, noise and security.

From the preceding discussions of Section III C – III E, following conclusions can be derived: (i) analog circuit designed with multi-V_{TH} transistors can retain original performance with appropriate resizing; and, (ii) in case of the wrong assumption of V_{TH} the performance will deteriorate significantly.

IV. Combined Design and Discussions

In this section, we integrate the components described in the previous section to study the proposed multi-V_{TH} design with respect to variability, overhead and RE effort. We also present a heuristic to extend the proposed design principle to other analog circuits.

A. Combined Multi-V_{TH} Design

Multi V_{TH} transistors can simultaneously be included in separate blocks discussed above. To investigate the performance of the combined design, we simulate the design with LVT MB1, MB3, ML3, M6T, and M6B. Fig. 6 shows that the open loop low-frequency gain drops about 98 dB, from 70.6 dB for base/secure design to -28.1 dB for adversarial observation with incorrect V_{TH}. The closed-loop gain is ~19.13 and THD is ~ 0.23%. However, with NVT the same circuit gives a closed-loop gain of 9.14×10^{-3} which is unusable.

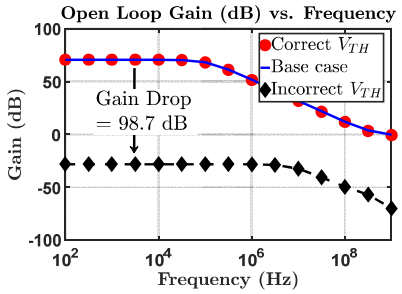


Fig. 6. Open loop gain comparison among baseline design, design with correct mixed V_{TH} and design with incorrect V_{TH}. Gain drops sharply for incorrect V_{TH}.

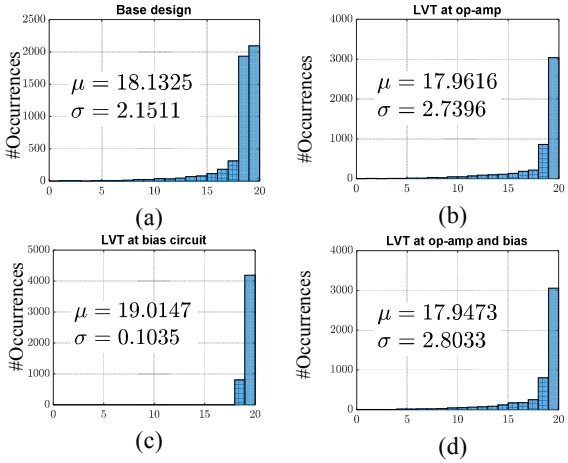


Fig. 7. Gain distribution due to threshold voltage mismatch: (a) baseline design, (b) LVT at op-amp, (c) LVT at the bias circuit and (d) LVT at both op-amp and bias.

B. V_{TH} Mismatch Analysis

The mismatch between the threshold voltages of two transistors may arise due to random dopant fluctuation and this might be more detrimental in a mixed-V_{TH} design. Therefore, we investigate the impact of process variation due to threshold voltage mismatch. According to Pelgrom's model, the variance of the difference in threshold voltage (V_{TH}) is given by the equation [35], [36]:

$$\sigma^2(\delta Vth) = \frac{A_{VTH}^2}{WL} + S_{VTH}^2 D_X^2 \quad (4)$$

Where $\sigma^2(\delta Vth)$ is the variance of the difference of threshold voltages between the transistors; A_{VTH} and S_{VTH} are the area and spacing proportionality constants for V_{TH}; W and L are the dimensions of each transistor; and D_X is the spacing between them. If the layout is done carefully, for example following common centroid approach, the mismatch is mostly dominated by the $A_{VTH}^2/(WL)$ [36]. A_{VTH} for our simulation is $4.5mV.\mu m$ [37]. We run Monte-Carlo simulation with variance calculated from (4). Secure design variation analysis is performed for three cases: (a) Bias generator: with LVT MB1 and MB3; (b) Op-amp: with LVT M6T, M6B, M3T and M4T and (c) Combined design: with LVT MB1, MB2, M6T, M6B, M3T and M4T. Corresponding base design is also simulated for comparative analysis. The results are shown in Fig. 7(a) – (d). It can be noted that the secure mixed-V_{TH} design worsens the mean up to 1% and standard deviation by 30%.

C. Overhead Analysis

The area overhead introduced by the proposed design mainly includes the transistor resizing due to V_{TH} change. Generally, LVT requires smaller (W/L) which leads to negative area overhead. On the hand, HVT design incurs positive overhead. Area overhead accounting is summarized in Table III for several cases. Considering area-overhead and performance LVT design can be chosen.

TABLE III. Area Overhead (A/O)
(Bold options are used in combined design)

Transistor(s)	V_{TH}	A/O	Transistor(s)	V_{TH}	A/O
MB1, MB3	**LVT**	**-1%**	MCM	LVT	-0.2%
	HVT	6.5%		HVT	5.76%
M6T, M6B	**LVT**	**-1.8%**	**ML3**	**LVT**	**-0.5%**
	HVT	48%		HVT	11.27%
M3T, M4T	LVT	-1.2%	Combined	-	-2.8%
	HVT	18.9%	-	-	-

D. Reverse Engineering Effort Analysis

In this test case, there are a total 55 transistors. However, considering pairing (e.g. MB1 and MB3; MB2 and MB4; M3T and M4T etc.) the effective number of transistors will be 47 and thus the adversary needs to check less number of permutations than the theoretical maximum. At this point, two paradoxical statements between Section II (i.e. pairing increases RE) and this section (i.e. pairing reduces the number of permutations thus reduces RE), needs to be understood. If V_{TH} change is not applied symmetrically in the paired transistors, then the adversary can spot anomalous transistor sizing and can break the design in one-shot. However, if the V_{TH} change is applied

in a pair, the number of required permutations will be less than the theoretical maximum ($3^{47}<3^{55}$). Assuming that adversary will require 0.1 seconds to validate each combination using automated script and simulator, the RE effort could be 0.1 sec $\times 3^{47} \approx 10^{13}$ years which is a large value (considering HSPICE runtime of 0.1 sec from our simulation).

For smaller designs, the RE effort can be increased by transistor splitting. For example, M6T and M6B transistors can each be split into two transistors (suppose, M6X1 and M6X2; X = T or B) in parallel while keeping their sizes equal after V_{TH} alteration of one or both transistors. Table IV shows that split design with correct V_{TH} retains original performance whereas for incorrect V_{TH} the gain drops and THD increases. This single splitting increases the effective number of transistors from 47 to 49. Thus, the RE increases to 0.1 sec $\times 3^{49} \sim 10^{14}$ years (10X higher). Splitting all transistors into two or more parallel branches can increase the RE effort by orders of magnitude.

It is to be noted, for binary key-based locking as in [14] and [15], RE effort varies as the power of 2 whereas for the proposed V_{TH} based obfuscation the effort varies as the power of 3 (3 V_{TH} choices). Therefore, RE effort is higher for the proposed method for the same value of N. Moreover, RE effort in [14] and [15] depends on key-size, N whereas effort in the proposed method depends on the number of the transistors, N, in the design. Therefore, for larger designs, RE effort inherently increases for the proposed method whereas in [14] and [15], to increase RE effort, additional key-bit has to be introduced which incurs relatively more area penalty.

TABLE IV. PERFORMANCE COMPARISON WITH SPLIT M6T AND M6B

Parallel transistors	W/L (V_{TH})	Correct Gain	Correct THD	Incorrect Gain	Incorrect THD
M6X1	13/2 (LVT)	19.14	0.19%	0.17	1.86%
M6X2	13/2 (NVT)				

E. Design Heuristic

The preceding discussions can be used to develop a heuristic for mixed V_{TH} based secure design. *First*, the designer has to pick-up performance critical *NVT* transistors to make those LVT/HVT. One good way to start is the biasing circuitry like reference current generator as it dictates the bias currents for subsequent blocks. Apart from the amplifier, many other analog designs like filters, oscillators, data converters etc. use

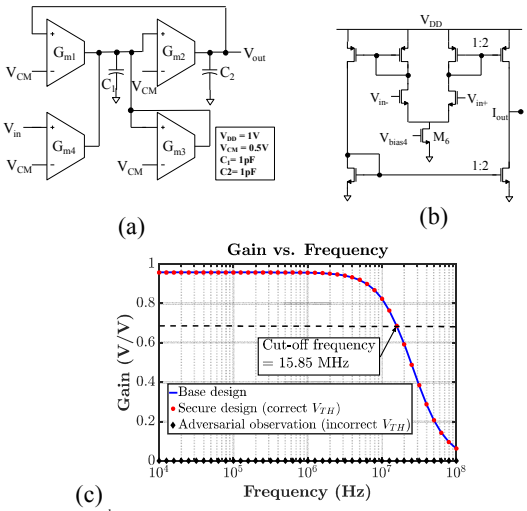


Fig. 8. (a) A 2nd order $G_m - C$ filter; (b) the operational transconductance amplifier (OTA) for realizing transconductance stages in (a). V_{bias4} for the OTA is generated from a similar bias network as in Fig. 3(a) and 3(b); (c) the frequency response of the filter.

reference current generator. Therefore, from a secure design stand-point, transistors in the reference current circuit can be replaced with LVT/HVT to mask reference current and gate voltages that will be used in subsequent blocks. *Second*, LVT/HVT transistors should be inserted in a pair if possible. For example, in Fig. 3(a), if MB1 is made LVT then it has to be resized to W/L = 20/2. With a resized MB1 and nominally sized MB3 (W/L = 60/2), the V_{biasp} will be at same level. However, the adversary can easily spot the size mismatch between MB1 and MB3 which are supposed to be equal sized and can trace back to V_{TH} mismatch between these two. Thus, the RE effort will be reduced. Therefore, V_{TH} change and resizing shall be done in a symmetric fashion and in a pair if possible.

F. Extending Design Heuristics to $G_m - C$ Filter

Amplifiers are sort of ubiquitous in different kind of analog designs e.g., data converters need comparators which are basically amplifiers, active filters etc. Therefore, the design heuristic developed in Section IV E along with preceding discussions can be extended to another class of analog circuit i.e., Transconductance (G_m) – C filter. Fig. 8(a) shows a 2nd

TABLE V. GAIN, THD AND (W/L) FOR SEVERAL SELECTED OPTIONS.

Reference current generator						M1T & M2T		LVT	NVT	HVT	NVT	**Bias voltage generator**					
		LVT	NVT	HVT	NVT		Gain	18.56	19.13	19.28	18.38			LVT	NVT	HVT	NVT
MB1 & MB3	Gain	19.13	0.72	19.12	15.6		THD	0.10	0.32	0.35	0.17	ML1	Gain	19.12	19.15	19.16	18.95
	THD	0.23	19.53	0.25	16.42		(W/L)	8/2	8/2	580/2	580/2		THD	0.24	0.21	0.20	0.38
	(W/L)	20/2	20/2	330/2	330/2	M3B & M4B	Gain	18.86	19.05	19.11	18.69		(W/L)	8/2	8/2	200/2	200/2
MB2 & MB4	Gain	19.17	19.03	19.10	19.16		THD	0.26	0.22	0.48	0.18	MR1	Gain	19.21	19.17	19.14	19.17
	THD	0.17	0.35	0.29	0.18		W/L	10/2	10/2	1200/2	1200/2		THD	0.18	0.15	0.15	0.16
	(W/L)	30/2	30/2	50/2	50/2	M3T & M4T	Gain	19.25	9.95m	18.94	0.33		(W/L)	10/10	10/10	10/10	10/10
Amplifier							THD	0.14	4.78	0.15	7.40	MR3	Gain	19.21	19.43	19.14	19.11
							W/L	12/2	12/2	840/2	840/2		THD	0.18	0.39	0.15	0.14
M1B & M2B	Gain	18.12	18.00	19.2	18.69	MCM	Gain	18.83	18.76	19.06	15.54		(W/L)	5/2	5/2	600/2	600/2
	THD	0.56	3.2653	0.38	0.63		THD	0.11	0.10	1.33	7.16						
	W/L	8/2	8/2	620/2	620/2		(W/L)	1/10	1/10	100/10	100/10						

*THD is in % and gain in (V/V).

order G_m – C filter implementation [38]. The transconductance stage is realized with an Operational Transconductance Amplifier (OTA) as in Fig. 8(b) [34]. Here, $G_{m1\text{-}4}$ are the transconductances of the OTAs. For this test case, all the transconductances are equal which makes the DC gain of the filter $G_{m4}/G_{m1} = 1$. The G_m – C filter is simulated with 50nm BSIM4 transistor models [39] with following V_{TH0} values: NVT = 220 mV, LVT = 70 mV and HVT = 370 mV. V_{bias4} for the OTA is generated from a biasing network similar to Fig. 3(a)-(b). Fig. 8(c) shows the frequency response of the filter for three different cases. The base design with all NVT transistors has a cut-off frequency of 15.8 MHz (C_1=C_2=1pF). In the secured design, transistor M6 of each OTA is replaced with a resized HVT transistor. The simulation results show the secured version has the same frequency response as the NVT base design. However, the adversarial duplication of the secured design, with all NVT transistors, behaves erratically with highly diminished pass-band gain as evident from the simulation results in Fig. 8(c) (diamond marker). There is a total of 52 transistors (16 in the bias + 36 in the filter) in this 2nd order G_m – C filter (38 effective transistors after considering pairing). A brute force attack will require 3^{38} trials leading to a reverse engineering effort of approximately 0.1 sec × 3^{38} ~ 10^9 years.

V. Conclusion

In this paper, a secure analog design methodology with multi V_{TH} transistors is proposed. Extensive performance and variability analysis are presented. Multi V_{TH} designs can secure the IP while retaining performance specifications. The proposed design can impose extremely high RE effort even for smaller analog design for brute-force analysis to identify the transistor V_{TH} and therefore, successfully discouraging the RE attacks.

Acknowledgment

The authors would like to thank Parvez Ahmmed from NCSU for helpful discussions on analog circuit and Sujay Hosur from PSU for helping with circuit diagrams.

References

[1] R. K. Lowry, "Counterfeit electronic components –an overview," Presented at the *Military, Aerospace, Space-borne, and Homeland Security (MASH) Workshop*, 2007.

[2] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, August 2011.

[3] Farinaz Koushanfar and Gang Qu. 2001. "Hardware metering", *In Proceedings of the 38th annual Design Automation Conference (DAC '01). ACM*, New York, NY, USA, 490-493.

[4] Koushanfar F., Qu G., Potkonjak M. (2001) Intellectual Property Metering. In: Moskowitz I.S. (eds) Information Hiding. IH 2001. Lecture Notes in Computer Science, vol. 2137. Springer, Berlin, Heidelberg.

[5] Yousra Alkabani *et al.*, "Remote activation of ICs for piracy prevention and digital right management," *2007 IEEE/ACM International Conference on Computer-Aided Design*, San Jose, CA, 2007.

[6] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", DAC, vol. 6, pp. 9-14, 2007

[7] A. Baumgarten, A. Tyagi, and J. Zambreno. "Preventing IC Piracy Using Reconfigurable Logic Barriers.", IEEE Design and Test of Computers.

[8] G. K. Contreras *et. al.*,"Secure Split-Test for preventing IC piracy by untrusted foundry and assembly," 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems.

[9] J. A. Roy, F. Koushanfar and I. L. Markov, "Ending Piracy of Integrated Circuits," in Computer, vol. 43, no. 10, pp. 30-38, Oct. 2010.

[10] [Online]:https://www.erai.com/CustomUploads/ca/wp/2013_4%20Counterfeiting%20and%20Semiconductor%20Value%20Chain%20Economics%20-%20Mr%20%20Rory%20King%20-%20IHS%20Inc.pdf

[11] R. Torrance and D. James, *The State-of-the-Art in IC Reverse Engineering*. Berlin, Heidelberg: Springer, 2009, pp. 363–381.

[12] Y. Bi, J. Yuan, and Y. Jin, "Beyond the Interconnections: Split Manufacturing in RF Designs," *Electronics*, vol. 4, no. 3, pp. 541–564.

[13] D. H. K. Hoe, J. Rajendran, and R. Karri, "Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors," in *Computer Society Annual Symposium on VLSI*, 2014, pp. 516–521.

[14] V. V. Rao and I. Savidis, "Protecting Analog Circuits with Parameter Biasing Obfuscation," in *Latin American Test Symposium*, 2017, pp. 1–6.

[15] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sánchez-Sinencio and J. Hu, "Thwarting analog IC piracy via combinational locking," *2017 IEEE International Test Conference (ITC)*, Fort Worth, TX, 2017, pp. 1-10.

[16] T. Adachi, A. Ishikawa, A. Barlow and K. Takasuka, "A 1.4 V switched capacitor filter," *IEEE Proceedings of the Custom Integrated Circuits Conference*, Boston, MA, 1990, pp. 8.2/1-8.2/4.

[17] S. S. Bazarjani and W. M. Snelgrove, "Low voltage SC circuit design with low -V_t MOSFETs," *Circuits and Systems, 1995. ISCAS '95., 1995 IEEE International Symposium on*, Seattle, WA, 1995, pp. 1021-1024 vol.2.

[18] K. Bult, "Analog design in deep sub-micron CMOS," *Proceedings of the 26th European Solid-State Circuits Conference*, Stockholm, Sweden.

[19] D. Buss, "Device issues in the integration of analog/RF functions in deep submicron digital CMOS," *International Electron Devices Meeting 1999. Technical Digest* , Washington, DC, USA, 1999.

[20] I. R. Nirmala, D. Vontela, S. Ghosh and A. Iyengar, "A novel threshold voltage defined switch for circuit camouflaging," *2016 21st IEEE European Test Symposium (ETS)*, Amsterdam, 2016, pp. 1-2.

[21] A. De and S. Ghosh, "Preventing Reverse Engineering using threshold voltage defined multi-input camouflaged gates," *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2017.

[22] B. Erbagci, C. Erbagci, N. E. C. Akkaya and K. Mai, "A secure camouflaged threshold voltage defined logic family," *2016 IEEE International Symposium on Hardware Oriented Security and Trust*.

[23] K. E. Khadiri and H. Qjidaa, "Integrated 60-V class-D power output stage with 95% efficiency in a 0.13µm SOI BCD process," *2015 Intelligent Systems and Computer Vision (ISCV)*, Fez, 2015, pp. 1-6.

[24] W. Vandervorst et al., "Spreading resistance roadmap towards and beyond the 70nm technology," in Journal of Vac. Sci. and Tech., 2002.

[25] N. Duhayon et al., "Assessing the performance of two-dimensional dopant profiling techniques," in Journal of Vac. Sci. and Tech., 2004.

[26] C. C. Williams, "Two-Dimensional Dopant Profiling by Scanning Capacitance Microscopy," in Annual Review of Materials Science, 1999.

[27] C. Sommerhalter et al., "High-sensitivity quantitative Kelvin probe microscopy by noncontact ultra-high-vacuum atomic force microscopy," in Applied Physics Letters, 1999.

[28] E. Volkl et al., "Introduction to electron holography," 1999.

[29] Y. Huang *et al.*, C. C. Williams, and H. Smith, "Direct Comparison of Cross sectional Scanning Capacitance Microscope Dopant Profile and Vertical Secondary Ion-mass Spectroscopy Profile," *Journal of Vacuum Science Technology*, 1996.

[30] V. Vartanian *et al.*, "Metrology Challenges for 45 nm Strained-Si Devices," *Characterization and Metrology for ULSI Technology*, 2005.

[31] M. V. Stangoni, "Scanning Probe Techniques for Dopant Profile Characterization," in *PhD Thesis*, 2005.

[32] P. De Wolf *et al.*, "Status and review of two-dimensional carrier and dopant profiling using scanning probe microscopy," in *Journal of Vac. Sci. and Tech.*, 2000.

[33] Predictive Technology Model. [Online]: http://ptm.asu.edu

[34] R. Jacob Baker. 2010. CMOS Circuit Design, Layout, and Simulation (3rd ed.). Wiley-IEEE Press.

[35] M. J. M. Pelgrom, H. P. Tuinhout and M. Vertregt, "Transistor matching in analog CMOS applications," *International Electron Devices Meeting 1998. Technical Digest (Cat. No.98CH36217)*, San Francisco, CA, USA.

[36] L. Pileggi, G. Keskin, X. Li, Ken Mai and J. Proesel, "Mismatch analysis and statistical design at 65 nm and below," *2008 IEEE Custom Integrated Circuits Conference*, San Jose, CA, 2008, pp. 9-12.

[37] STMicroelectronics. [Online]: http://st.com

[38] Adel S. Sedra and Kenneth C. Smith. Microelectronic Circuits Revised Edition (7th ed.). Oxford University Press, Inc., New York, NY, USA.

[39] [Online]: http://cmosedu.com/cmos1/cmosedu_models.txt