Energy and Area Aware Digital Fingerprint Generator Using Intrinsic Randomness

Jawar Singh, Sandeepkumar Pandey and Pramod K Tiwari

May 3, 2019

Energy and Area Aware Digital Fingerprint Generator Using Intrinsic Randomness

Sandeepkumar Pandey
Department of Electronics Engineering,
Shri Ramdeobaba College of Engineering and Management,
Nagpur, India, 440013
Email:pandeys@rknec.edu

Jawar Singh and Pramod K Tiwari
Department of Electrical Engineering,
Indian Institute of Technology Patna,
Bihar, India, 801106
Email:(jawar, pktwari)@iitp.ac.in

***Abstract*—Manufacturing variability/fluctuations is a major concern in integrated circuits and this has been exploited to design a hardware security primitive or digital fingerprint generator, referred as physical unclonable function (PUF) for resource constrained low power applications. The proposed architecture employs single transistor as PUF cell, one operational amplifier (OpAmp), and little peripheral circuitry, thereby making it very light and suitable for resource constrained applications. Simulation results show that the energy consumption of proposed design is 30fJ/bit which is 6.33× lesser than earlier reported design, it has 0.0025μm^2 area/bit and the values of 1s and 0s are equi-probable with probability of a '1' being 50.2%. The mean measured by inter HD plot is 49.72 which is very close to an ideal value of 50%. This affirms that the proposed PUF can supply unique identifiers.**

***Keywords*—Physical Unclonable Function (PUF), Security, Low energy consumption, Digital fingerprint.**

I. Introduction

Aggressive scaling of CMOS technology, two major sources of process variations manifest themselves in the form of sub-wavelength lithographic variation and variations resulting from vacillations in quantity and locality of dopant atoms [2]–[4]. Random Dopant Fluctuation (RDF) and Line Edge Roughness (LER) influence the threshold voltage (V_T) of the MOSFET, which in turn becomes a random function. This random function could be exploited to generate a hardware circuitry and whose electrical properties are unique and driven by physical traits of MOSFETs called PUF. These are emerging hardware security primitive circuits widely used for secret key generation, identification, and authentication of electronic devices. Different approaches and various topologies for PUF realization have been studied and proposed in the literature. Published PUF implementations could broadly be classified as: SRAM based PUFs, arbiter PUFs, RO (Ring Oscillator) PUFs, and optical PUFs [5]–[8].

However, main challenges associated with PUF designs include: relatively small challenge space, high resource utilization, power consumption, and susceptibility to modeling attacks. Particularly, the PUF architectures proposed in [9]–[11] have high resource utilization overhead. This presents serious bottleneck in resource constrained designs. We propose a PUF architecture which extracts and amplifies the process variations outlined above to generate secret keys. The proposed PUF is evaluated on important performance matrices of standard PUF design and it is observed that our design has extremely low power and resource utilization.

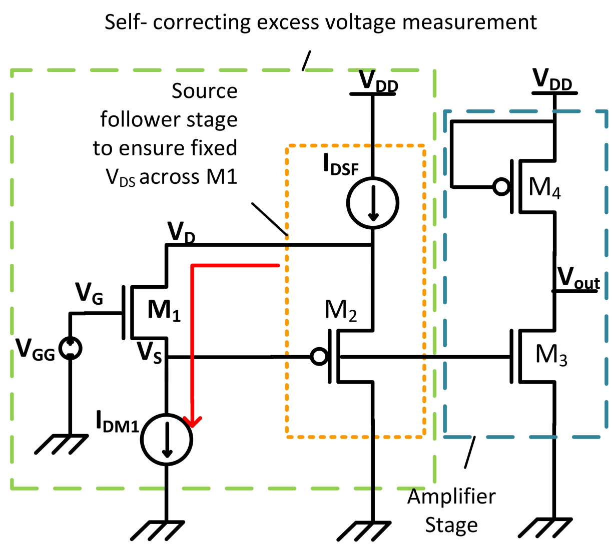

Fig. 1. Self-correcting overdrive voltage tracking along with amplifier stage.

II. Self-correcting overdrive voltage tracking circuit along with amplifier stage

We propose a PUF architecture which extracts and amplifies the random fluctuations or intrinsic randomness that arises during manufacturing of integrated circuits to generate secret keys. A sub-threshold CMOS PUF cell is proposed as shown in Fig. 1, where, transistor (M_1) is used to extract process fluctuations and made to operate in sub-threshold region by applying appropriate (V_{GG}) and (I_{DM1}). The reason of operating M_1 in sub-threshold region is that process fluctuations are dominant and related to overdrive voltage ($V_{GS} - V_T$) that yields percentage variation in (I_{DS}) versus (V_{GS}) higher in this region. Also the transistors M_3 and M_4 of amplifier stage, as shown in Fig. 1 are operated in sub-threshold region to have lower energy dissipation.

If we ensure constant V_{DS} and I_{DS} through M_1 then, the overdrive voltage would be constant. However, random fluctuation in V_T forces the V_{GS} for self-correction to keep ($V_{GS} - V_T$) constant. In other words, random fluctuation in (V_T) of M_1 is translated to change in (V_{GS}) and later amplified by the amplifier stage for secret key generation. In Fig. 1, a constant current I_{DM1} through M_1 is set and the source follower ensures fixed V_{DS} across M_1. If the (V_T) of the M_1 changes then so does the source voltage thereby keeping the term $(V_{GS} - V_T)$ as constant. Since threshold voltage fluctuation is random in nature, we can say that V_{GS} variation is random too. For array of such devices whose (V_T) is assumed to vary randomly due to process fluctuations and same is extracted for generation of secret keys. The extracted randomness in the form of source voltage variation in correspondence with (V_T) variation is further amplified by the presented amplifier stage comprising of M_3 and M_4. The I_{DS} in sub-threshold region changes exponentially with V_{GS}. Therefore, V_S gets amplified at V_{out}. Node voltage V_S corresponds to the sensed change in threshold voltage which is amplified by amplifier stage. The voltage variation at V_S are such that it never goes beyond the threshold voltage of M_3. This means that M_3 always operates in sub-threshold region. The amplifier stage is designed to improve the voltage swing available at V_S. The gain of the amplifier has been obtained analytically using small signal equivalent model of amplifier in [18], as shown in Fig. 2. Due to small variation at node V_S, the gain is expressed as:

$$\frac{v_{\text{out}}}{v_s} = g_{mM3}\left(r_{oM3}//r_{oM4}\right) \tag{1}$$

Because of sub-threshold operation, the current is expressed as [19]:

$$I_{sub} = A \times e^{(V_{gs}-V_{th0}-\gamma V_{sb}+\eta V_{ds})/mv_T} \times \left(1 - e^{(-V_{ds}/v_T)}\right) \tag{2}$$

where,

$$A = \mu_0 C_{ox}\frac{W}{L_{eff}}v_T^2 e^{1.8} \tag{3}$$

μ_0 is carrier mobility, η is the drain induced barrier lowering (DIBL) coefficient, γ is the body effect coefficient, m is the sub-threshold swing coefficient of the transistor and V_T is the thermal voltage. From (2) the small signal parameters i.e g_m, r_o are calculated as

$$g_{mM3} = \frac{\partial I_{ds}}{\partial V_{gs}} = \frac{\partial I_{ds}}{\partial V_S} = \frac{I_{ds}}{m_{nM3}v_T} \tag{4}$$

$$r_{oM3} = \frac{1}{\frac{\partial I_{ds}}{\partial V_{ds}}} = \frac{1}{\frac{\eta_{M3}I_{ds}}{m_{M3}v_T}} \tag{5}$$

$$r_{OM4} = \frac{1}{\frac{\partial I_{ds}}{\partial V_{ds}}} = \frac{1}{\frac{\eta_{M4}I_{ds}}{m_{M4}v_T}} \tag{6}$$

by combining (1) , (4) , (5) , (7), we get:

$$\frac{v_{\text{out}}}{v_s} = \frac{m_{M4}}{m_{M3}\eta_{M3} + m_{M3}\eta_{M4}} \tag{7}$$

The length of the transistor M_3 and M_4 is used for gain enhancement of amplifier stage since it modifies the respective DIBL coefficients.

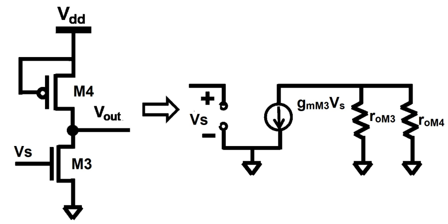

Fig. 2. Small signal equivalent circuit of the amplifier stage.

III. The PUF architecture of secret key generation

The complete PUF architecture of secret key generation is shown in Fig. 3. This is based on the self-correcting excess voltage tracking circuit described in Fig. 1. Challenges are applied to row and column decoders based on which a particular device is selected. The applied row challenges select the gate of row transistors R_i (i=1,2,3,...N), such that the source voltage V_{SX} (x=1,2,3,...N) gets applied to the input of source follower circuit. The same gets applied to the amplifier stage for amplification. The output of source follower circuit is applied to the non-inverting input of the OpAmp. The other input (inverting) of the OpAmp is obtained from V_{DX} (x=1, 2, 3, 4, 5,..N). For example the applied challenge to the row decoder and column is such that it internally selects row-0 and column-4 so that C_4=0, C_{4bar}=1 and R_0=1. This selects the green colored transistor in dashed ellipse, as shown in Fig. 3. Fixed constant current I_{DSM} is made to flow through the path OpAmp-V_{D1}-V_{S1}-ground. This is shown with red arrow in Fig. 3, and corresponding flow of current is as shown in Fig. 1 with same red color arrow. Source follower and OpAmp together ensure that the constant V_{DS} is applied to the green transistor (or any other selected device). Also the current source I_{DMN} ensures constant current is applied through the selected transistor. Hence, the random process variations in threshold voltage are available at node V_{S1} in the Fig. 3 that is further amplified by amplifier stage and given to key storage register through buffer circuit. The switching threshold of the buffers is designed at half of the swing available at the output of the amplifier stage. Complete process for secret key generation is shown step-by-step in Fig. 4 with the help of a flow chart. Therefore, random but consistent outputs are generated out of the buffer circuit which is stored in the secret key storage register.

More popular PUF architectures such as delay-based PUFs are prone to modeling attacks, because their basic building topologies can be mathematically represented by model whose unknown delay coefficients can be estimated by machine learning techniques from the gathered challenge-response pairs. Our proposed PUF directly uses a random amount of V_T fluctuation available in manufacturing process. This will make it more resilient to attacks. The single transistor selection for random V_T extraction employs a two dimensional array structure addressed by row and column decoders. This increases the challenge response space. For proposed PUF with M challenge bits applied at the row decoder for row selection and N challenge bits applied at the column decoder for column selection, there could be 2^MX2^N challengeresponse pairs. This satisfies the criterion for strong PUF. The proposed architecture selects one

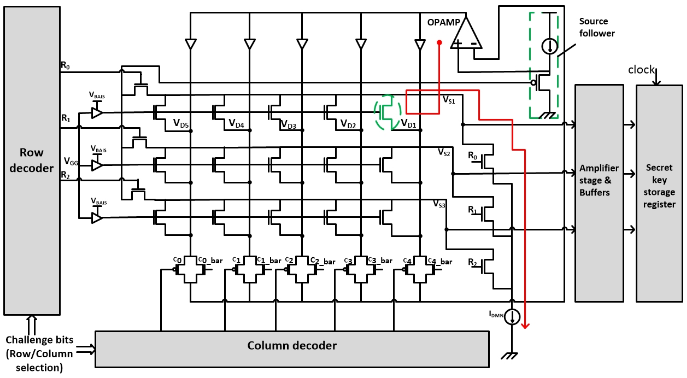

Fig. 3. Architecture of proposed PUF. Challenge bits are applied to row/column decoder to select a particular transistor. A fixed I_{DMN} and V_{DS} are applied to the device and source voltage V_S is read and applied to buffer to get the secret keys.

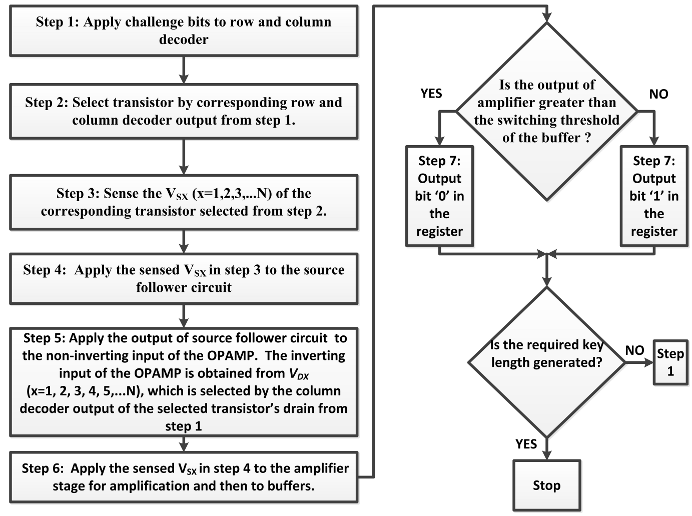

Fig. 4. Flow chart of the proposed PUF architecture for generation of challenge response pair.

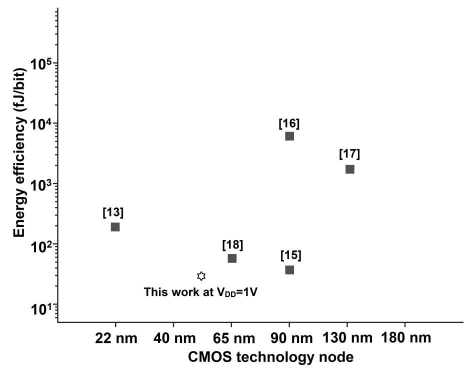

Fig. 5. E_{bit} comparison with CMOS PUFs. At nominal operating condition the proposed PUF achieves an E_{bit} of 30 fJ/bit.

transistor at a time for secure bit generation. Thus, required variable key lengths could be generated based on platform requirements and computational constraints.

The threshold voltage (V_T) fluctuations or the mobility (μ) fluctuations during fabrication are the two MOSFET parameters which could be effectively used to realise PUFs. Since these parameters show local fluctuations due to statistical fluctuations. Our PUF working in the sub-threshold region is characterized by the V_T variations of the selected MOSFETs. The V_T can be expressed as a function of temperature as [20]:

$$V_T(T) = V_T(T_0) \cdot (1 + TCV_T \cdot (T - T_0)) \tag{8}$$

where V_T is measured at the temperature T_0 and the temperature coefficient of V_T is defined as:

$$TCV_T = \frac{1}{V_T} \cdot \frac{\partial V_T}{\partial T} \tag{9}$$

In our PUF design, temperature dependence can be compensated by varying the bias current with temperature. Thus, V_{GS} changes corresponding to V_T changes in selected transistors could be made to stay constant with varying temperature.

IV. Simulation Results

All the simulation results are obtained from 50 nm CMOS technology models with V_{DD}=1V. The energy consumption E_{bit} of the proposed PUF is evaluated as: E_{bit} = I_{drawn} X V_{DD}/f_{clk}, where, I_{drawn} is the current drawn from supply to produce the response bit, V_{DD} is the supply voltage, and f_{clk} is the applied clock frequency. The circuit draws 30nW for 1us for one bit generation thereby giving E_{bit} of 30fJ/bit which is 6.33X lesser than [12]. A comparison of energy efficiency of the proposed PUF design with the earlier reported PUF designs is shown in Fig. 5. At the nominal operating condition, the proposed PUF achieves an E_{bit} of 30 fJ/bit. The size the PUF is defined by area per bit. Since the size depends on the technology strongly, the area is expressed in F^2/bit, where F is the minimum features size. It is the square of the minimal channel length. The proposed PUF has 0.0025μm^2 area/bit.

The proposed architecture employs single transistor as a PUF cell, only one OpAmp and very little processing (peripheral) circuitry thereby making it ultra-light. The threshold voltage variation is assumed to be Gaussian distribution for Monte-Carlo analysis. For PUF output to be non-predictable, the values of 1s and 0s should be equal-probable. Fig. 6 shows the response (uniformity) of 64 bit PUF output for 100 runs. The probability of a '1' is 50.2%. This equal-probable occurrence 1s and 0s makes the response our PUF difficult to anticipate, and therefore, resistant to attacks.

Uniqueness is another very important security metric for PUF. The quality of a given PUF instance to provide an unambiguously distinct behavior in comparison with different other PUFs with the identical topology implemented on different chips is measured by this quantity. Suppose the two PUFs (each with a challenge response pair (CRP) of 6 bits are to be realized on two distinct chips. When both the PUFs are subjected to same challenge say (010101) then the response obtained from each PUF is distinct. Assuming the Hamming distance between obtained response is 2, which implies that 25% of the response bits differ. Ideally Uniqueness should be close to 50%. Fig. 7 shows the inter Hamming distance (HD) of die for one thousand runs. The mean measured by inter HD plot, as shown in Fig. 7 with mean of 49.72 which is very close to an ideal value of 50%. This affirms that the proposed PUF can supply unique identifiers.

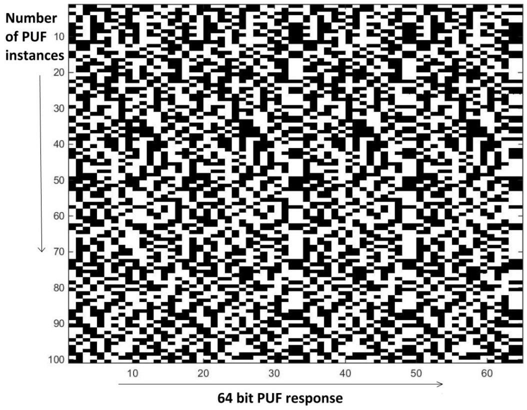

Fig. 6. Uniformity in PUF response. 0 is represented by white pixel and '1 is represented by black pixel for 64X100 PUF response bits.

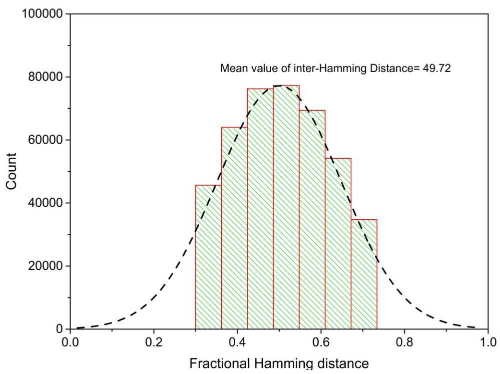

Fig. 7. Inter Hamming distance plot for 1000 Monte-Carlo runs.

V. Conclusion

The proposed PUF design relies on concept of the self-correcting overdrive voltage tracking circuit. The design is low power and the only power hungry component used is OpAmp. It could be switched off after particular transistor outputs are identified. Thus, significantly reducing the power consumption. The PUF cell used as source of randomness is minimum sized transistor making the area per bit matrix of proposed cell extremely small. The proposed PUF architecture has low hardware overhead in terms of input/output and processing circuitry. The proposed architecture employs single transistor as PUF cell, only one OpAmp and very little processing circuitry thereby making it ultra-light weight which is well suited for resource constrained applications. The circuit draws 30nW for 1us for one bit generation thereby giving energy dissipation of 30fJ/bit.

References

[1] Hee-Gook Lee, Soo-Young Oh and G. Fuller, "A simple and accurate method to measure the threshold voltage of an enhancement-mode MOSFET," in IEEE Transactions on Electron Devices, vol. 29, no. 2, pp. 346-348, Feb. 1982. doi: 10.1109/T-ED.1982.20707

[2] Lars W. Liebmann "Resolution enhancement techniques in optical lithography: It's not just a mask problem", Proc. SPIE 4409, Photomask and Next-Generation Lithography Mask Technology VIII, (5 September 2001). doi: 10.1117/12.438332;

[3] R. W. Keyes, "Effect of randomness in the distribution of impurity ions on FET thresholds in integrated electronics," in IEEE Journal of Solid-State Circuits, vol. 10, no. 4, pp. 245-247, Aug. 1975. doi: 10.1109/JSSC.1975.1050600.

[4] Xinghai Tang, V. K. De and J. D. Meindl, "Intrinsic MOSFET parameter fluctuations due to random dopant placement," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 5, no. 4, pp. 369-376, Dec. 1997. doi: 10.1109/92.645063

[5] D. E. Holcomb, W. P. Burleson and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," in IEEE Transactions on Computers, vol. 58, no. 9, pp. 1198-1210, Sept. 2009. doi: 10.1109/TC.2008.212

[6] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA, 2004, pp. 176-179. doi: 10.1109/VLSIC.2004.1346548

[7] V. P. Yanambaka, S. P. Mohanty, E. Kougianos and J. Singh, "Secure Multi-key Generation Using Ring Oscillator Based Physical Unclonable Function," 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Gwalior, 2016, pp. 200-205. doi: 10.1109/iNIS.2016.053

[8] Ravikanth Pappu, Ben Recht, Jason Taylor, Neil Gershenfeld, "Physical One-Way Functions," in Science, Vol. 297, Issue 5589, pp. 2026-2030, 20 Sep 2002 doi: 10.1126/science.1074376

[9] S. Tao and E. Dubrova, "Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS," in Electronics Letters, vol. 52, no. 10, pp. 805-806, 12 5 2016. doi: 10.1049/el.2016.0292

[10] T. Dhar and A. R. Trivedi, "Area and energy-efficient physically unclonable function based on k-winners-take-all," in Electronics Letters, vol. 52, no. 24, pp. 1978-1980, 24 11 2016. doi: 10.1049/el.2016.1991

[11] Z. Wang, Y. Chen, A. Patil, C. Chang and A. Basu, "Current mirror array: A novel lightweight strong PUF topology with enhanced reliability," 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, 2017, pp. 1-4. doi: 10.1109/ISCAS.2017.8050476

[12] S. K. Mathew et al., "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), San Francisco, CA, 2014, pp. 278-279. doi: 10.1109/ISSCC.2014.6757433.

[13] K. Agarwal, S. Nassif, F. Liu, J. Hayes and K. Nowka, "Rapid Characterization of Threshold Voltage Fluctuation in MOS Devices," 2007 IEEE International Conference on Microelectronic Test Structures, Tokyo, 2007, pp. 74-77. doi: 10.1109/ICMTS.2007.374458

[14] M. Majzoobi, G. Ghiaasi, F. Koushanfar and S. R. Nassif, "Ultra-low power current-based PUF," 2011 IEEE International Symposium of Circuits and Systems (ISCAS), Rio de Janeiro, 2011, pp. 2071-2074. doi: 10.1109/ISCAS.2011.5938005

[15] S. Stanzione, D. Puntin and G. Iannaccone, "CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," in IEEE Journal of Solid-State Circuits, vol. 46, no. 6, pp. 1456-1463, June 2011. doi: 10.1109/JSSC.2011.2120650

[16] Y. Su, J. Holleman and B. P. Otis, "A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations," in IEEE Journal of Solid-State Circuits, vol. 43, no. 1, pp. 69-77, Jan. 2008. doi: 10.1109/JSSC.2007.910961

[17] J. Li and M. Seok, "Ultra-Compact and Robust Physically Unclonable Function Based on Voltage-Compensated Proportional-to-Absolute-Temperature Voltage Generators," in IEEE Journal of Solid-State Circuits, vol. 51, no. 9, pp. 2192-2202, Sept. 2016. doi: 10.1109/JSSC.2016.2586498

[18] M. Meterelliyoz, P. Song, F. Stellari, J. P. Kulkarni and K. Roy, "Characterization of Random Process Variations Using Ultralow-Power, High-Sensitivity, Bias-Free Sub-Threshold Process Sensor," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 8, pp. 1838-1847, Aug. 2010. doi: 10.1109/TCSI.2009.2037449

[19] A. Chandrakasan, W. J. Bowhill, and F. Fox, Design of High-Performance Microprocessor Circuits. Piscataway, NJ: IEEE Press, 2000

[20] Baker, R. J. (2008). CMOS: circuit design, layout, and simulation. Piscataway, NJ, IEEE Press.