Energy-Efficient Near-Threshold Standard Cell Library for IoT Applications

AbdelRahman Hesham[1], Amin Nassar[1], and Hassan Mostafa[1,2]
[1]Electronics and Communications Engineering Department, Cairo University, Egypt.
[2]University of Science and technology, Nanotechnology and Nanoelectronics Program, Zewail City of Science and Technology, October Gardens, 6th of October, Giza 12578, Egypt.
{*a.heshamm@gmail.com, amin.nassar@yahoo.com, hmostafa@uwaterloo.ca*}

***Abstract*—In this paper, a low-energy minimum-area CMOS standard cell library suitable for IoT applications is proposed. Energy consumption reduction is achieved by operating the library in Near-Threshold Voltage (NTV) region, and by designing layout of cells at the minimum possible area for the used technology process. Body biasing technique is proposed to boost pMOS performance. Operating voltage and transistor sizing are also selected to achieve the minimum energy consumption while operating at the frequency range of 1MHz to 20MHz which is suitable for IoT applications. The proposed library was designed and characterized in UMC 130 nm CMOS technology process. The library was modeled to be used in synthesis tools. To prove the benefit for IoT applications, the library was benchmarked by implementing 3 cryptographic algorithms: ASCON, AEGIS-128, and AEZ. Synthesis results are showing that the three cores can operate at 18 MHz, 14 MHz, and 16 MHz respectively, while consuming 0.466 pJ, 3.006 pJ, and 5.064 pJ.**

***Index Terms*—CMOS digital integrated circuits, design methodology, near-threshold CMOS circuits, ultra-low power design, ultra-low energy, IoT, ASCON, AEGIS, AEZ**

I. Introduction

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless communication. This is resulting in a wide range of applications touching every aspect of our life, like wearable devices, connected cars, and smart homes. Enablement of IoT spread is depending on the reliability of devices accessing it. Device reliability is based on: (1) computation power, (2) efficiency of energy consumption, and (3) security against possible threats.

Computation power of IoT devices has been widely explored in the literature [1]–[5], with a major interest in energy reduction techniques. These techniques have been explored and proposed at all design levels; namely circuit, logic, RTL, algorithm, and system levels. For IoT devices, most of energy saving is achieved by circuit-level solutions. One of the most growing topics in this area is the feasibility of voltage scaling to reduce energy consumption. Circuit design in subthreshold region has gained increasing interest to achieve low power requirements by operating the circuits at the Minimum Energy Point (MEP) [1]. The drawback of this MEP paradigm is the significant loss in performance [2]. To recover some of the performance loss while maintaining the power gains, Near-Threshold Voltage (NTV) operation was introduced [2]. It was shown that in NTV, energy savings can be in the order of 10X, with only a 10X degradation in performance, providing a much better energy/performance trade-off than subthreshold operation [3].

In addition to computation power and energy concerns in IoT applications, the possible threats deriving from widespread adoption of such a technology are stressed. As predicted by Cisco, there will be 50 billion IoT connected devices by 2020 [6]. Integration of such a tremendous number of devices into IoT potentially brings in a new concern, System Security. Thus, cryptography became one of the main approaches to secure and overcome attacks on user data. Significant research effort was done to provide algorithmic level cryptography solutions and to assess hardware implementation of these algorithms. In [7], ASIC implementation of 3 commonly used cryptography algorithms is conducted to check their suitability for IoT applications. Similarly, architectural solutions are proposed in [8] and used to implement co-processor suitable for Narrow-Band (NB) IoT devices. Also, in this direction and in 2012, the European Network of Excellence in Cryptology (ECRYPT) called for a new competition for authenticated ciphers: CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) [9]. Review of hardware implementation of CAESAR algorithms are presented in [10], [11]. The winning algorithms were announced in 2019, and they were covering 3 main areas of application: lightweight, high performance, and defense-in-depth. In this paper, 3 of these applications were explored for potential benefit in IoT devices.

In this paper, a low-energy minimum-area standard cell library is proposed in UMC 130 nm process. Library is operating in NTV region at 350 mV supply. This supply was selected to achieve the minimum Power Delay Product (PDP) for the used process node. The minimum area is achieved by minimizing cell height and by utilizing Euler's Path in design of each cell layout. A calculation method is proposed to get minimum cell height as a function of technology parameters. The Inverse Narrow Width Effect (INWE) was checked and utilized for library PPA gains. The proposed library is showing better energy and area measurements compared to other libraries surveyed. To show the gains from utilizing NTV operation, the library is benchmarked against a commercial library operating in Super-Threshold Voltage region to implement three of CAESAR finalists: ASCON [12], AEGIS-128 [13], and AEZ [14].

The rest of the paper is organized as follows. Section II describes the library architecture design and discusses the proposed solutions for improving library PPA. Then,comparison result with similar library is presented. Section III describes the flow used for designing the set of cells constructing the library. Section IV reports the benchmark results of the proposed library using cryptography IPs. Lastly, the paper is concluded in Section V.

II. Library Architecture Design

In digital design using standard-cell approach, all modules must have the same height [15], [16]. The placement of standard cells has to be aligned with some pre-specified standard-cell rows in the placement region. And because of its popularity, most placement algorithms assume a standard-cell design style. The minimum cell dimensions or in other words the minimum resolution of cell placement in 2D area is defined as Unit Tile. All the cells in standard-cell library have to be of –or multiples of– unit tile height and to have a width that is a multiple of unit tile width.

A. Minimum Cell Height Design

Here, we are proposing a method to define the minimum cell height for a given process node. All the drawings inside cell must meet the Design Rule Checks (DRC). And given that the shapes drawn inside any cell are from Front-End Of Line (FEOL) layers or Back-End Of Line (BEOL) layers, rules related to both layer groups must be considered.

The process parameters needed for FEOL checks are: minimum diffusion enclosure inside NPLUS ($\mathrm{EN_n}$), minimum diffusion enclosure inside PPLUS ($\mathrm{EN_p}$), minimum diffusion width inside NPLUS ($\mathrm{W_n}$), and minimum diffusion width inside PPLUS ($\mathrm{W_p}$). From Fig. 1, the minimum cell height ($\mathrm{H_{min,FEOL}}$) is calculated as:

$$H_{min,FEOL} = 2EN_p + 2EN_p + W_n + W_p \qquad (1)$$

Then, to calculate $\mathrm{H_{min}}$ from BEOL rules, we need to construct the layout given in Fig. 2. The limitation here is coming from the first metal layer (metal 1). (1) Any metal 1 shape must keep a spacing distance of $\mathrm{S_{m1}}$ to other metal 1 shapes, (2) any via connecting metal 1 to poly shape or diffusion shape (CONT) must be enclosed by metal 1 shape, and finally (3) PG rails needs to be drawn on metal 1 to provide supply voltage to transistors. The minimum PG rail width is the minimum metal 1 width ($\mathrm{W_{m1}}$). So:

$$H_{min,BEOL} = 4S_{m1} + 3CE_{m1} + W_{m1} \qquad (2)$$

In order to avoid any routing problem, either internally to connect transistors, or externally when the cell gets connected to other cells, cell height must be integer multiples of the pitch of the first horizontal metal layer -metal 2 in our proposed library- ($\mathrm{P_{m2}}$).

$$H_{min} = nP_{m2} \qquad (3)$$

And from Equations (1), (2), (3), we can define:

$$n = max(H_{min,FEOL}, H_{min,BEOL})/P_{m2} \qquad (4)$$

where n is the minimum cell architecture tracks for a given technology. This equation is technology-independent, and can be applied to planar CMOS process nodes.

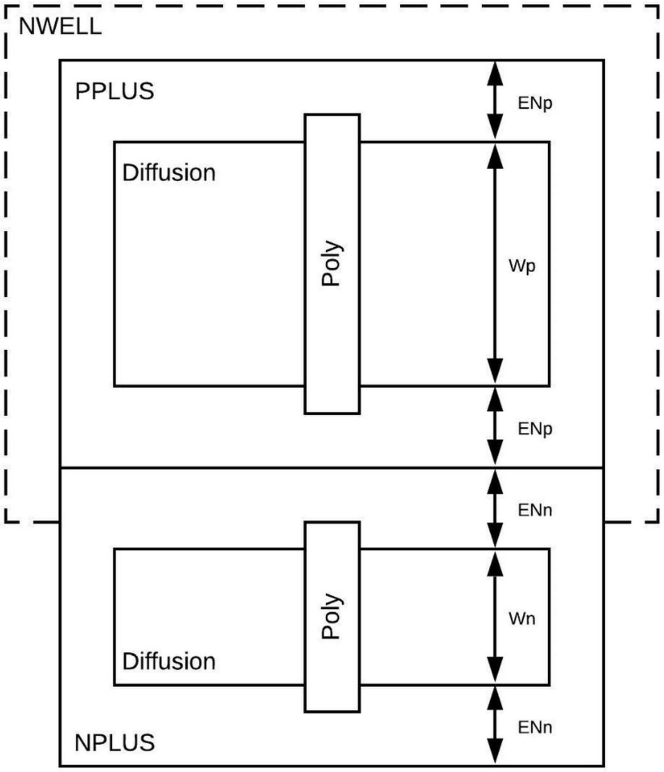

Fig. 1. Technology FEOL parameters to calculate minimum tracks.

For UMC 130nm process, and based on the process Design Rule Manual (DRM), the minimum cell height tracks is calculated to be 5T. This is the minimum number of tracks reported in the literature. In [17], a 6T architecture is developed, in [18]–[21] 8T–12T architectures are developed by utilizing multi-finger structure to achieve more area efficiency.

B. Cell Layout Design

Implementation of 5T architecture is enabled by: using Euler's path theory for layout design, and using 3 metal layers for intra-cell routing.

Euler's path theory [22]–[24] is used in [25] to provide the minimum-area transistor placement inside given cell area. The resulting transistor placement can be routed in multiple ways. The selected routing of each cell used in our library considers: (1) pin accessibility when used in Placement and Routing tools, (2) minimizing pin capacitance, and (3) meeting technology DRC rules. Three metal layers are used for intra-cell routing. Metal 1 and metal 2 are used extensively, while metal 3 is rarely used when all metal 1 and metal 2 resources are used.

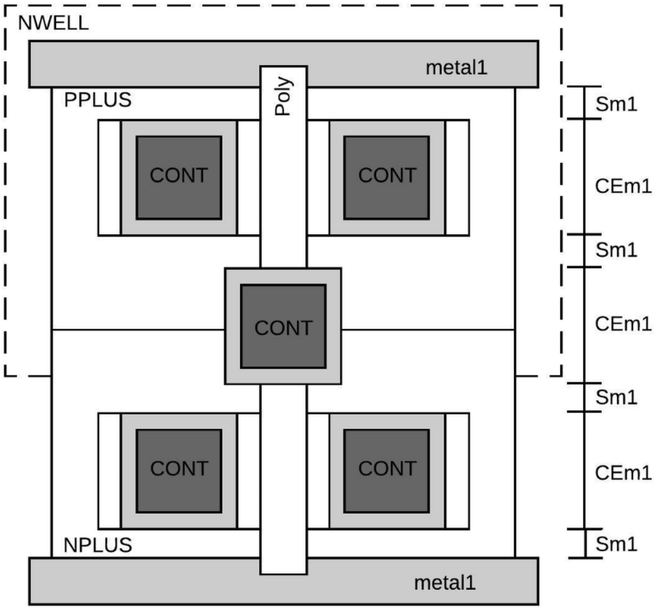

Fig. 2. Technology BEOL parameters to calculate minimum tracks.

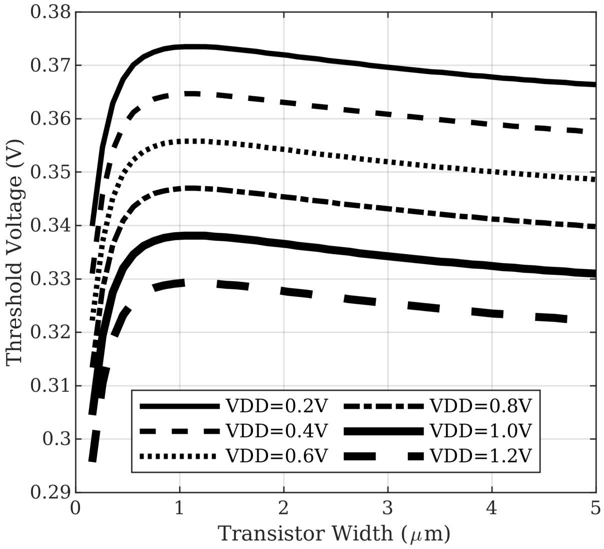

Fig. 3. NMOS threshold voltage vs transistor width at different supply voltages in 130 nm.

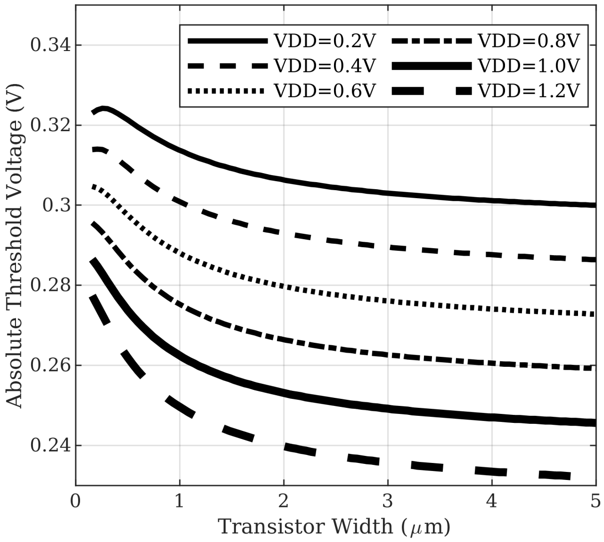

Fig. 4. PMOS absolute threshold voltage vs transistor width at different supply voltages in 130 nm.

C. Transistor Sizing

Transistor sizing is one of the main factors deciding the library power and speed performance. The used 5T architecture sets a limit on the maximum transistor sizing:

$$W_n + W_p \leq 5P_{m2} - 2EN_p - 2EN_n \tag{5}$$

For the used process, this limit is calculated to be 1.04 μM. This value is allowing transistor sizing in the range around and beyond minimum pMOS and nMOS widths.

Literature was explored for the different transistor sizing techniques in NTV region in order to improve performance with the minimum impact on power. The Inverse-Narrow-Width Effect (INWE) was introduced in [26] as the reduction in the threshold voltage due to reduction in transistor width, allowing for higher driving currents. INWE can be utilized to achieve performance gain while operating in the NTV. [18] has used the minimum pMOS and nMOS finger widths to maximize INWE while having the minimum threshold voltage. [18] has shown the INWE in 90 nm, 65 nm, and 45 nm process nodes. In Fig. 3 and Fig. 4, the INWE impact in 130 nm process node is shown, which aligns with the previously introduced results for NMOS. For PMOS, the INWE is not significant. As shown in Fig. 4, a slight reduction in threshold voltage near the minimum width is noticed while reducing supply voltage. So, sizing PMOS at minimum width is not as important as NMOS. This was also shown for 180 nm in [27]. Also, from Fig. 4, W_p needs to be >350 nm to avoid the threshold voltage curve peak, but increasing it too much will not improve performance due to increase in fanout load.

D. pMOS Body Biasing Technique

In order to balance the NMOS and PMOS currents and to reduce the difference between rise and fall times without increasing PMOS size, body biasing technique is used. The conventional body-biasing used in digital circuits is done by connecting n-well to the supply voltage and connecting p-substrate to the ground. This technique is cancelling the body effect, hence, the dependence of threshold voltage on the body voltage is not noticed. This technique is used in superthreshold region, and can be used also for NTV region [28]. In [29] the low-voltage swapped body biasing (LVSB) was used in 180 nm at 0.5 V, where the n-well and p-substrate voltages are swapped compared to the conventional biasing. The technique used in [28] is compromising between the conventional technique and the LVSB one. In this technique, the body terminals of all nMOS and pMOS devices are connected together without supply or ground connections. The proposed technique in this paper is to connect only pMOS body to the ground. With this way, the forward body biasing provides significant performance gain for the pull-up network, while keeping the pull-down one at the same power consumption.

E. Testing and Supply Selection

Inverter INV_X1 was created with W_n set to 160 nm, the minimum width available, and with pMOS body terminal connected to ground. A Fanout-of-4 (FO4) test-bench for the inverter cell was created to simulate the impact of transistor sizing and body biasing on delay, power, and PDP. Fig. 5 and Fig. 6 are showing that, the proposed body biasing is providing better performance with slight increase in power in the subthreshold and nearthreshold regions when compared to conventional biasing. This is not the case as the supply voltage increases, where power starts to grow faster. Supply voltage is selected to be 350 mV, where the performance gain is achieved at the cost of power increase while achieving the same PDP as of the conventional body biasing. This supply voltage is selected at the center of flat range in PDP curve to allow for PVT margins while having the same value.

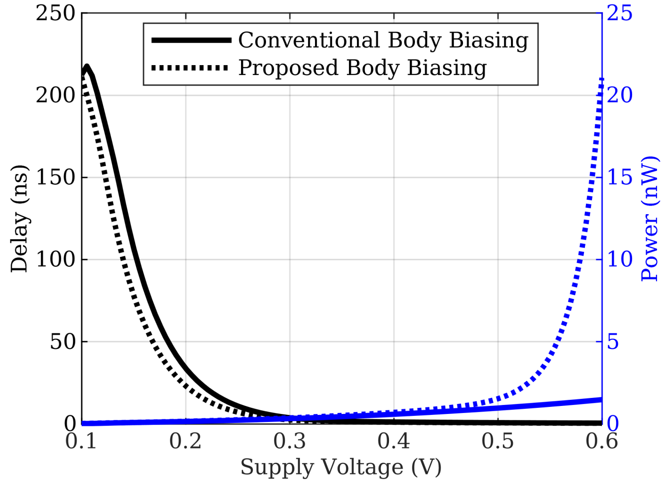

Fig. 5. Inverter power and delay vs the supply voltage.

F. Literature Comparison

In this section, comparison with other work is provided. In Table I, comparison is done with a 6T NVT library designed in 130 nm operating at 400 mV. Comparison is held for the nominal corner: TT, nominal supply, and room temperature of 25°C. Although our proposed library is lagging in delay by about 3X, it is achieving better PDP by about 2000X.

III. Cell Design Flow

The list of cells included in proposed library are covering the basic functions to build any design; namely combinational cells (e.g. INV, AND, OR, NAND, NOR, XOR, and XNOR) and sequential cells (e.g. D-Flipflop and D-Latch). The flow used is shown in Fig. 7. For each cell, static CMOS implementation is selected, which is needed to provide Rail-to-Rail swing with the low supply used. Then, a test-bench is created to check circuit functionality and to measure its timing and power parameters. Once passed, design is transformed into its layout implementation. Qualified layout needs to pass essential physical verification checks, namely DRC and LVS. Then, design functionality and specifications are rechecked to avoid any corruption due to layout design. SPICE model describing our cell is then generated. This model is passed to cell characterization and modeling flow, which creates the library model needed for synthesis tools. The generated model includes all cell delay information, in addition to cell power performance. This view is essential input to logic synthesis process. Proposed library model was generated using Synopsys Siliconsmart tool. The tool takes cell SPICE model as input, and based on user configuration, it generates the cell model in .LIB format.

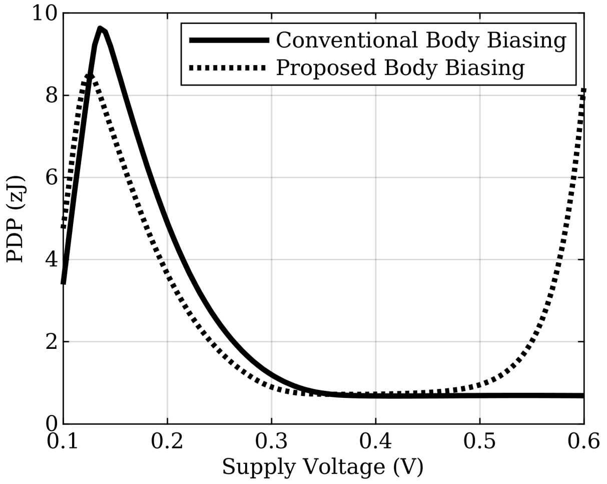

Fig. 6. Inverter PDP vs the supply voltage.

TABLE I
Power, Delay, and PDP comparison between proposed 5T library and Similar 6T library

Library cell	**Delay, ns**		**Power, nW**		**PDP, fJ**	
	Proposed	***Lib1***[a]	***Proposed***	***Lib1***	***Proposed***	***Lib1***
INV_X1	3.59	0.96	0.117	-	0.000421	1.432
ND2_X1	3.99	1.24	0.127	-	0.000506	1.605
NR2_X1	3.6	1.2	0.215	-	0.000754	1.522

[a] 6T NTV library implemented in 130 nm [17].

IV. Library Benchmarking

In this section, comparison results are provided to show the power and performance gains of proposed library. Table II is showing the ratio of frequency lost by moving from superthreshold to subthreshold region. In Table III, power and frequency were explored considering process, voltage,

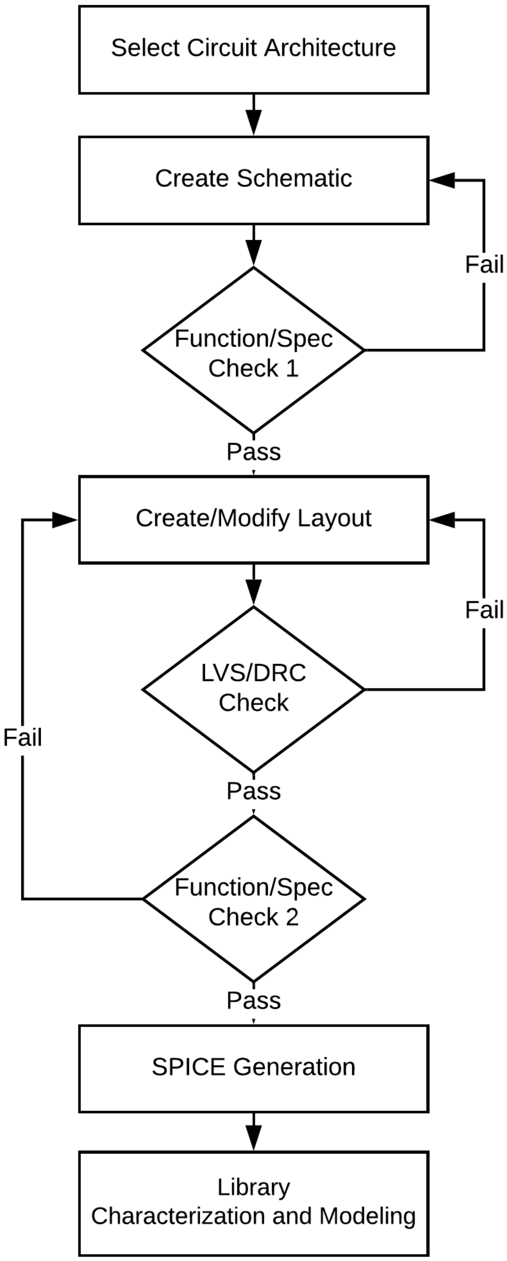

Fig. 7. The Used Cell Design Flow.

and temperature (PVT) variations. A 10% supply variation is considered. The worst performance corner found to be SS0p315vm40c with about 16X reduction from nominal one. The worst power consumption corner is found to be FF0p385v125c with about 10X increase compared to nominal one.

Finally, in Table IV, implementation of cryptographic cores is done. In the final portfolio of the CAESAR competition [30], ASCON was selected as the primary choice for lightweight authenticated encryption, and AEGIS-128 was selected as the primary choice for high performance authenticated encryption. AEZ is another algorithm that was one of the finalists in the same competition. Assessment of the library was done by comparing synthesis results of the three designs using the proposed Near-Threshold library compared to using a commercial library operating in Super-Threshold region at the same technology node. The used RTL implementations are the ones used for CAESAR candidates benchmarking [31].

TABLE II
MAXIMUM FREQUENCY COMPARISON WITH FOUNDRY COMMERCIAL LIBRARY

Tested Core	Max Frequency, MHz		Ratio of Frequency Loss
	Proposed Library	***Commercial Library***	
ASCON	18	330	18.33
AEGIS-128	14	100	7.14
AEZ	16	125	7.81

TABLE III
LIBRARY POWER AND FREQUENCY ACROSS PVT CORNERS

Corner	**Internal (nW)**	**Switching (nW)**	**Leakage (nW)**	**Total (nW)**	**Max Freq**
TT0p35v25c	62.547	2.1999	6.1509	70.896	16
SS0p315vm40c	2.07	0.079	61.5	2.22	1
SS0p315v125c	4.13	0.165	19.0	23.7	5
FF0p385vm40c	295	9.86	2.29	307.0	52
FF0p385v125c	383.1	12.0	808	1203	67

V. CONCLUSION

The proposed Near-Threshold standard cell library is showing significant energy saving when used in essential applications in IoT. This energy saving comes at the cost of frequency reduction. The paper has provided solutions to find optimal Power-Performance-Area operating point. A technology-dependent methodology is proposed for minimum standard cell layout architecture design. INWE was utilized in addition to a proposed body biasing technique that boosts performance in NVT. Three of the latest and best cryptographic cores are considered in this paper for benchmarking the proposed library. Quality of improvement can be measured as the ratio of energy improvement and frequency reduction. ASCON archives a ratio of 1.7, while AEGIS-128 achieves a ratio of 2.5, and finally AEZ achieves a ratio of 4.1. Still, the achieved frequencies are sufficient for IoT applications.

VI. ACKNOWLEDGMENT

This work was partially funded by ONE Lab at Zewail City of Science and Technology and at Cairo University, NTRA, ITIDA, ASRT, and NSERC.

REFERENCES

[1] A. Wang, and A. Chandrakasan, "A 180-mV Subthreshold FFT Processor Using a Minimum Energy Design Methodology," IEEE JOURNAL OF SOLID-STATE CIRCUITS, vol. 40, pp. 310–319, January 2005.

[2] B. Zhai, S. Pant, L. Nazhandali, S. Hanson, J. Olson, A. Reeves, M. Minuth, R. Helfand, T. Austin, D. Sylvester, and D. Blaauw, "Energy-Efficient Subthreshold Processor Design," IEEE Trans. On VLSI Systems, vol. 17, no. 8, pp. 1127–1137, Aug. 2009.

TABLE IV
POWER AND ENERGY COMPARISON AT TYPICAL CORNER BETWEEN PROPOSED LIBRARY AND FOUNDRY LIBRARY

Parameter	**ASCON @ 18 MHz**		**AEGIS-128 @ 14 MHz**		**AEZ @ 16 MHz**	
	Proposed	***Lib2***[a]	***Proposed***	***Lib2***	***Proposed***	***Lib2***
Internal Power (microns)	6.3108	203.4	26.262	576.7	62.547	2143
Switching Power (microns)	1.2718	70.198	14.471	281.2	2.1999	136.7
Leakage Power (microns)	0.7979	0.053527	7.3638	0.44421	6.1509	0.42639
Total Power (microns)	8.3804	273.7	48.097	858.3	70.896	2280.1
Internal Energy (microns)	0.465578	15.20556	3.006063	53.64375	5.064	162.8643
Ratio of Energy Gain	32.65954		17.84519		32.16119	

[3] R. Dreslinski, M. Wieckowski, D. Blaauw, D. Sylvester, and T. Mudge, “Near-Threshold Computing: Reclaiming Moore’s Law Through Energy Efficient Integrated Circuits,” Proceedings of the IEEE, vol. 98, no. 2, pp. 253–266, Feb. 2010.

[4] H. Reyserhove and W. Dehaene, “A 16.07pJ / cycle 31MHz Fully Differential Transmission Gate Logic ARM Cortex M0 core in 40nm CMOS,” 2016 IEEE European Solid-State Circuits Conference (ESSCIRC), pp. 257–260, 2016.

[5] Y. Bai, Y. Song, M. Bojnordi, A. Shapiro, E. Ipek and E. Friedman, “Architecting a mos current mode logic (mcml) processor for fast low noise and energy-efficient computing in the near-threshold regime,” ICCD, pp. 527–534, Oct 2015.

[6] D. Evans, “The Internet of Things How the Next Evolution of the Internet Is Changing Everything,” Cisco White Paper, 2011.

[7] M. Bahnasawi, A., K. Ibrahim, A. Mohamed, M. Khalifa, A. Moustafa, K. Abelmonim, Y. ismail, and H. Mostafa, “ASIC-Oriented Comparative Review of Hardware Security Algorithms for the Internet of Things Applications”, IEEE International Conference on Microelectronics (ICM 2016), Cairo, Egypt, pp. 285-288, 2016.

[8] SM. A. Sharaf, E. Abdelbary, H. Mostafa, “Efficient ASIC Implementation of a NB-IoT Security Co-Processor”, IEEE International MidWest Symposium on Circuits and Systems (MWSCAS 2020), Springfield, MA, USA, In Press.

[9] European Network of Excellence in Cryptology, “DIAC – Directions in Authenticated Ciphers, Jul. 2012. [Online]. Available: http://hyperelliptic.org/DIAC/ [Accessed: Apr. 25, 2020].

[10] N. Samir, A. S. Hussein, M. Khaled, A. N. ElZeiny, M. Osama, H. Yassin, A. Abdelbaky, O. Mahmoud, A. Shawky, and H. Mostafa, “ASIC and FPGA Comparative Study for IoT Lightweight Hardware Security Algorithms”, Journal of Circuits, Systems, and Computers (JCSC), vol. 28, no. 12, pp. 1-13, 2019.

[11] S. Sharaf, and H. Mostafa, “A Study of Authentication Encryption Algorithms(POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, AES-GCM) For Automotive Security”, IEEE International Conference on Microelectronics (ICM 2018), Sousse, Tunisia, pp. 315-318, 2018.

[12] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schlaffer, “Ascon v1.2: Submission to the CAESAR Competition,” Submissions to Round 3 of the CAESAR competition, 2016.

[13] H. Wu , and B. Preneel, “AEGIS: A Fast Authenticated Encryption Algorithm v1.1,” Submissions to Round 3 of the CAESAR competition, 2016.

[14] V. T. Hoang, T. Krovetz, and P. Rogaway, “Robust Authenticated-Encryption AEZ and the problem that it solves,” Oct. 2014. [Online]. Available: https://web.cs.ucdavis.edu/ rogaway/aez/rae.pdf [Access-ed: Apr. 25, 2020].

[15] Z. W. Jiang, H. Chen, T. C. Chen, Y. W. Chang, “Challenges and solutions in modern VLSI placement.,” 2007 International Symposium on VLSI Design Automation and Test VLSI-DAT 2007 - Proceedings of Technical Papers, 2007.

[16] K. Shahookar, P. Mazumder, “VLSI cell placement techniques,” ACM Comput. Surveys, vol. 23, no. 2, pp. 143–220, 1991.

[17] Y. W. Lim, N. A. Kamsani, R. M. Sidek, S. J. Hashim, and F. Z. Rokhani, “Six-track multi-finger standard cell library design for near-threshold voltage operation in 130nm complementary metal oxide semiconductor technology,” IET Circuits Devices Syst., 2019, Vol. 13 Iss. 5, pp. 710–716.

[18] Zhou, J., Jayapal, S., Busze, B., et al., “A 40nm dual-width standard cell library for near/sub-threshold operation,” IEEE Trans. Circuits Syst. I, Regul. Pap., 2012, 59, (11), pp. 2569–2577.

[19] Li, M.Z., Ieong, C.I., Law, M.K., et al.: “Energy optimized subthreshold VLSI logic family with unbalanced pull-up/down network and inverse narrow-width techniques,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 2015, 23, (12), pp. 3119–3123.

[20] Morris, J., Prabhat, P., Myers, J., et al.: “Unconventional layout techniques for a high performance, low variability subthreshold standard cell library,” IEEE Computer Society Annual Symp. on VLSI (ISVLSI), Bochum, 2017, pp. 19–24.

[21] Jun, J., Song, J., Kim, C.: “A near-threshold voltage oriented digital cell library for high-energy efficiency and optimized performance in 65nm CMOS process,” IEEE Trans. Circuits Syst. I, Regul. Pap., 2018, 65, (5), pp. 1567–1580.

[22] R. Bar-Yehuda, J. A. Feldman, R. Y. Pinter, and S. Wimer, “Depth-first-search and dynamic programming algorithms for efficient cmos cell generation,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol. 8, no. 7, pp. 737–743, 1989.

[23] K.Roy, “Optimum Gate Ordering of CMOS Logic Gates Using Euler Path Approach: Some Insights and Explanations,” Journal of Computing and Information Technology, CIT 15, pp. 85–92, 2007.

[24] S. W. Cheng and K. H. Cneng, “Modified Euler Path Rule For MOS Layout Minimization,” The 2004 IEEE Asia-Pacific Conference on Circuits and Systems, pp. 541–544, 2004.

[25] X. Xu, N. Shah, A. Evans, S. Sinha, B. Cline and G. Yeric, “Standard cell library design and optimization methodology for ASAP7 PDK: (invited paper),” 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 999–1004, Nov. 2017.

[26] L.A. Akers, M. Sugino, J.M. Ford, “Characterization of the inverse-narrow-width effect,” Electron Devices IEEE Transactions on, vol. 34, no. 12, pp. 2476–2484, 1987.

[27] M.-Z. Li et al., “Energy optimized subthreshold VLSI logic family with unbalanced pull-up/down network and inverse narrow-width techniques,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 12, pp. 3119–3123, Dec. 2015.

[28] W. Zhao, Y. Ha and M. Alioto, “Novel Self-Body-Biasing and Statistical Design for Near-Threshold Circuits With Ultra Energy-Efficient AES as Case Study”, IEEE Transaction on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 8, pp. 1390–1401, Aug. 2015.

[29] S. Narendra, J. Tschanz, J. Hofsheier, B. Bloechel, S. Vangal, Y. Hoskote, et al., “Ultra-low voltage circuits and processor in 180 nm to 90 nm technologies with a swapped-body biasing technique”, IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, pp. 156–157, 2004.

[30] D. J. Bernstein, “CAESAR Submissions,” Feb. 2019. [Online]. Available: https://competitions.cr.yp.to/caesar-submissions.html [Accessed: Apr. 25, 2020].

[31] K. Gaj, “Athena: Automated Tool for Hardware Evaluation,” Feb. 2019. [Online]. Available: https://cryptography.gmu.edu/athena [Accessed: Apr. 25, 2020].