

# Design and Security Evaluation of Negative Capacitance FETs for Energy Efficient and DPA Attack Resilient PRESENT-80 Block Cipher Design at Scaled $V_{DD}$

Renuka Chowdary Bheemana\*, Penumalli Koteswara Rao\*, *Member, IEEE*, Aditya Japa\*\*, *Member, IEEE*,  
Siva Sankar Yellampalli\*, *Senior Member, IEEE*, Ramesh Vaddi\*, *Senior Member, IEEE*

\*Department of Electronics and Communication Engineering, SRM University, Andhra Pradesh, India-522503

\*\*Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Telangana, India  
Emails: [renuka\\_chowdary@srmap.edu.in](mailto:renuka_chowdary@srmap.edu.in), [koteswara\\_p@srmap.edu.in](mailto:koteswara_p@srmap.edu.in), [aditya.japa@klh.edu.in](mailto:aditya.japa@klh.edu.in), [sivasankar.y@srmap.edu.in](mailto:sivasankar.y@srmap.edu.in),  
[ramesh.v@srmap.edu.in](mailto:ramesh.v@srmap.edu.in).

**Abstract**— Negative capacitance Field Effect Transistor (NCFET) is a promising CMOS compatible technology that exhibits relatively lower subthreshold swing (SS) and higher ON current at scaled  $V_{DD}$ . This paper for the first time explores the design and security evaluation of NCFET based ultra-light weight PRESENT-80 cipher at 0.5V  $V_{DD}$ . The NCFET based PRESENT-80 cipher is analyzed by varying the ferroelectric thickness ( $t_{fe}$ ) of NCFET device. NCFET based PRESENT-80 exhibit energy efficiency at  $t_{fe}$  of 4nm. At 0.5V, NCFET based PRESENT-80 at  $t_{fe}$  of 4nm exhibits 3.2× lower energy consumption compared to baseline 40nm CMOS design with 100MHz operating frequency. Apart from this, the security of NCFET based PRESENT-80 is evaluated against differential power analysis (DPA). With non-linear variation of dynamic power consumption profile, NCFET based PRESENT-80 is proved to be resilient against DPA compared to the baseline MOSFET design.

**Keywords**— *Negative capacitance field effect transistor (NCFET), Differential Power Analysis (DPA), Energy efficiency, Hardware security, Light weight cryptography, PRESENT-80 Cipher.*

## I. INTRODUCTION

Negative capacitance FET (NCFET) is a rapidly emerging technology that demonstrates subthreshold swing lesser than 60mV/dec through internal voltage amplification [1-2]. This is achieved by exploring ferroelectric (FE) material inside the gate stack and it is fully compatible with existing CMOS fabrication process [3]. Leveraging this process, NCFET circuits can operate with higher clock frequencies at lower supply voltages [4]. Numerous studies have been proposed divergent device architectures that achieve steep subthreshold swing, higher ON current and lower leakage compared to existing CMOS technology [5-6]. A recent study demonstrated that utilizing broad junctions and complementary capacitance matching, NCFET has achieved a hysteresis free behavior with steep subthreshold swing of less than 5mV/dec [7]. In addition, a PZT ferroelectric based low power and high performance 14nm NCFET is designed that can operate at ultra-low supply voltage of 0.24V [8]. Because of this enhanced performance, several researchers explored NCFETs to design digital circuits [9-11]. NCFET based Manchester carry chain adder and carry-look-

ahead adder have reported lower switching energy consumption compared with the existing FinFET counterpart [9]. Negative capacitance based ternary logic shown higher performance without additional footprint. Exploring hysteresis of NCFETs, compact non-volatile flip-flop is designed that exhibit lower energy consumption [10]. NCFET based multi-core with same micro-architecture, but different FE thickness has shown 8.3% better performance and 20% higher power-efficiency compared to existing heterogeneous multi cores [11]. On the other hand, NCFET is exploited to boost the analog circuit performance [12-14]. NCFET based common source amplifier is designed in negative differential resistance region that achieve 25% higher gain [12]. Leveraging NCFET steep slope and higher output impedance characteristics, a clock comparator and voltage-to-time converter is designed that achieve enhanced speed and linearity [13]. Additionally, taking the advantage of negative differential resistance in NCFETs, a hybrid OTA is designed that achieve remarkable improvement in the open-loop gain, the power supply rejection ratio, and the common-mode rejection ratio [14]. Apart from this, 1T-ferroelectric NOR type memory design demonstrated a simple erase, program, and read operations with ultra-low power consumption [15]. Further, 18× speed enhancement is observed in NCFET based compute-in SRAM compared to CMOS SRAM designs [16].

Although NCFET based circuits/systems have shown higher performance, the security of them need be verified against several hardware attacks due to the highly vulnerable internet of things (IoT) era [17-18]. However, very less works has shown NCFET technology benefits towards hardware security and further research is required to obtain more insights

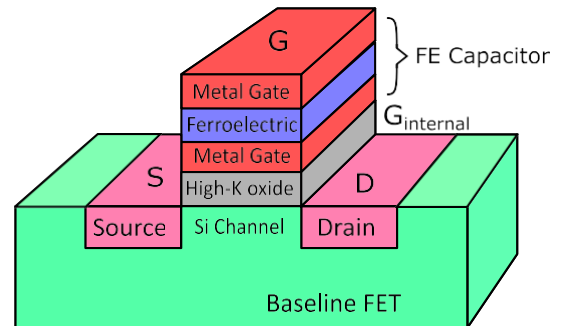


Fig. 1 NCFET device structure showing the integration of FE capacitor with baseline MOSFET.

of NCFETs for hardware security applications [19-20]. To obtain the full promise of NCFET, this paper proposes NCFET based

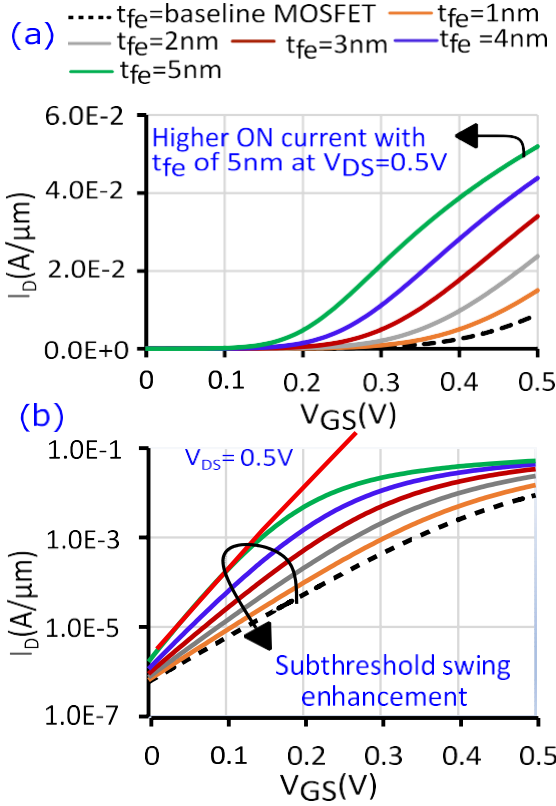


Fig. 2 NCFET (a)  $I_D$ - $V_{GS}$  characteristics demonstrating higher ON current (b)  $I_D$ - $V_{DS}$  with log scale on y-axis showing steep subthreshold swing.

Table 1 Performance comparison of NCFET device performance with MOSFET

Performance parameter	NCFET ( $t_{fe}=5\text{nm}$ )	NCFET ( $t_{fe}=4\text{nm}$ )	NCFET ( $t_{fe}=3\text{nm}$ )	Baseline MOSFET
ON current ( $\mu\text{A}/\mu\text{m}$ )	443	358	266	69.8
Leakage current ( $\text{nA}/\mu\text{m}$ )	2.62	3.21	3.68	4.64
$I_{ON}/I_{OFF}$ ratio	$168.5 \times 10^3$	$111.5 \times 10^3$	$72.3 \times 10^3$	$15.04 \times 10^3$
Subthreshold Swing (mV/dec)	49	56	63	99

ultra-light weight cipher design and security evaluation. This work for the first time presents the design, analysis and security evaluation of NCFET based PRESENT-80 cipher design.

## 2. NCFET device model and Characteristics

The NCFET device model considered in this work integrates ferroelectric (FE) capacitor and baseline MOSFET as shown in Fig. 1. FE material is used in the construction of the FE capacitor, which is sandwiched between two metallic layers. In order to represent FE capacitors and the standard Si-MOSFET, the Intel 40 nm p-type/n-type bulk FET model is explored in this model. This compact model captures several divergent

characteristics and several researchers explored to demonstrate NCFET based circuits/system [21-22]. The detailed parameters of FE material and baseline MOSFET can be found in [23]. The n-channel NCFET's drain current ( $I_D$ ) characteristics are shown in Fig. 2 alongside baseline MOSFET's gate-to-source voltage ( $V_{GS}$ ) characteristics (with  $t_{fe}$  ranging from 1nm to 5nm) (with  $t_{fe}$  of 0nm). Fig. 2(a) shows  $I_D$ - $V_{GS}$  varying  $V_{GS}$  from 0V to 0.5V. The NCFET with  $t_{fe} = 5\text{nm}$  achieves 6.4x higher ON current compared to baseline MOSFET. Moreover, NCFET exhibits steep subthreshold swing and lower leakage current compared to baseline MOSFET as shown in Fig. 2(b). As can be shown, compared to baseline MOSFET, NCFET with  $t_{fe} = 5\text{nm}$  achieves steep subthreshold swing (49mV/dec) and 1.77 lower leakage current. Table 1 summarises the performance comparison between NCFET and MOSFET devices.

## 3. Design and Security evaluation of NCFET based PRESENT-80

PRESENT is a 64-input substitution-permutation block cipher network with 80-bits or 128-bits key [24]. Due to the limited battery budgets of IoT devices, several applications use light-weight 80-bit key based PRESENT for encryption (PRESENT-80). The proposed NCFET PRESENT-80 is implemented in Cadence-Virtuoso environment by exploring 45nm NCFET

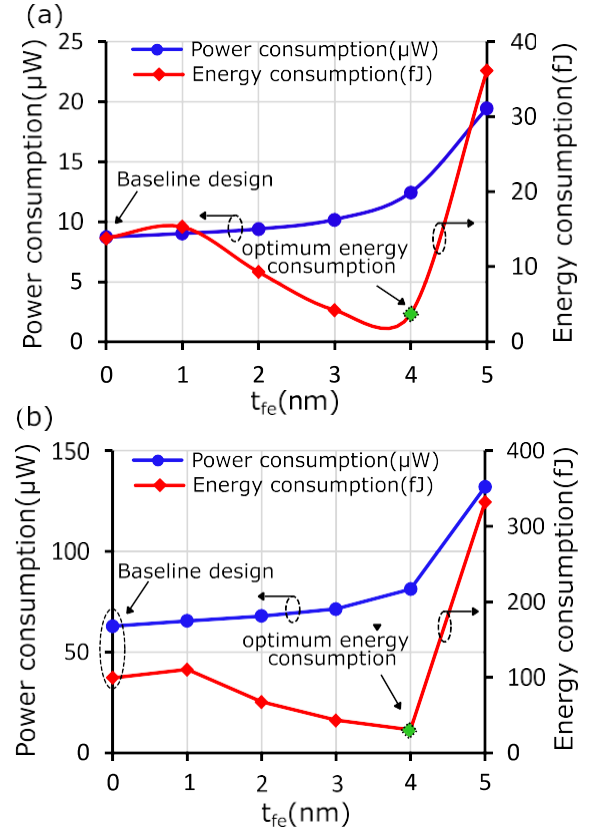


Fig. 3 Energy consumption and power consumption of NCFET based PRESENT-80 by varying  $t_{fe}$  (a) Operating at 10MHz (b) Operating at 100MHz.

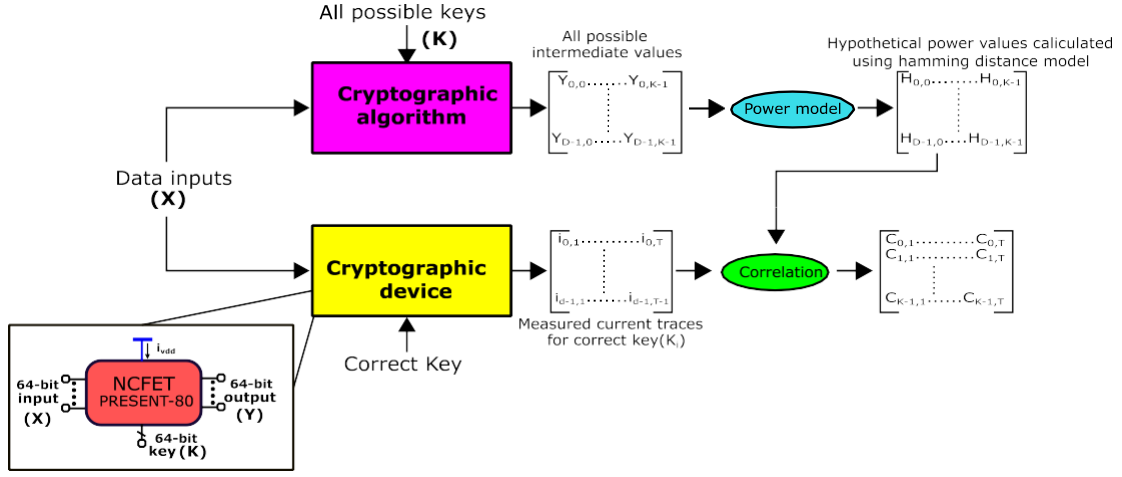


Fig. 4 DPA attack mechanism for NCFET based PRESENT-80 S-box design at  $V_{DD}=0.5V$

Verilog-A model [22] and the PRESENT-80 architecture [24]. Fig. 3 illustrates the proposed NCFET-based PRESENT-80's power and energy usage when adjusting  $t_{fe}$  at a supply voltage of 0.5V. With an increase in  $t_{fe}$ , the energy consumption of NCFET of the PRESENT-80 decreases, and it rises with  $t_{fe}$  greater than 4nm. When compared to baseline designs, the power consumption of the NCFET Present-80 shows negligible increase. NCFET design exhibits linear increment in power consumption and with  $t_{fe}$  beyond 4nm, the exponential increment in power consumption is observed. This is because the NCFET demonstrates enhanced device performance with an increase in  $t_{fe}$  (up to 4nm), which lowers the overall energy consumption of NCFET PRESENT-80. Beyond 4nm, due to the large increment in dynamic power consumption (with increased overall capacitance), the overall power consumption and energy consumption have increased exponentially. As demonstrated in Fig.3(a), NCFET PRESENT-80 with  $t_{fe}$  4nm shows 3.7x lower energy Consumption compared to the baseline MOSFET designs. Similar to this, as shown in Fig. 3(b), at an operating frequency of 100MHz, NCFET with 4nm  $t_{fe}$  demonstrates 3.2x lower energy usage than baseline designs. It is clear from this that the NCFET PRESENT-80 exhibits its best energy efficiency at a  $t_{fe}$  of 4nm.

Apart from the lower energy consumption, this work evaluates the robustness of PRESENT-80 against DPA attack. The S-box design in PRESENT-80 is responsible to create non-linearity and produces the cipher text. Due to this, S-box design [23] is considered to evaluate the security of PRESENT-80 against DPA. Fig. 4 demonstrates the procedure of DPA on PRESENT-80 S-box design. Following this procedure, DPA is conducted on PRESENT S-box design. Upon applying several inputs, the current traces have been recorded with an original key  $K=6$ . The sample current traces obtained from the baseline PRESENT-80 S-box and NCFET PRESENT-80 S-box at a supply voltage of 0.5V are shown in Fig. 5. In contrast to CMOS S-box, the current traces of NCFET S-box are seen to be random. As a result, NCFET architecture displayed data independent current traces in contrast to CMOS S-box. This randomness or mismatch is due to the non-linearity obtained from increased gate capacitance of NCFET. The current traces changed when NCFET gate capacitance rose because dynamic power consumption is a function of gate capacitance.

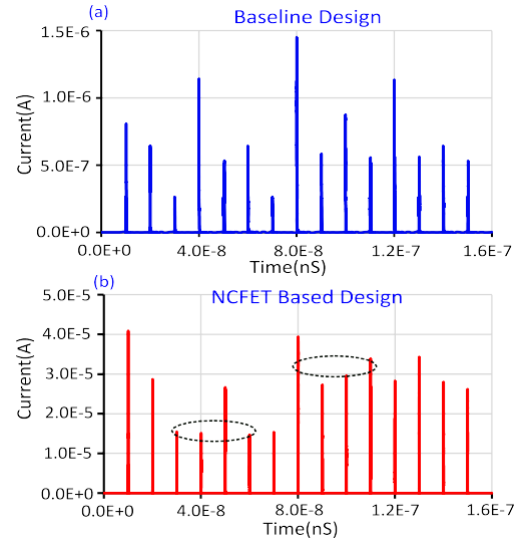


Fig. 5 Power Profile comparison of NCFET PRESENT S-box design with baseline 40nm CMOS PRESENT S-box design at  $V_{DD}=0.5V$ .

Fig. 6 displays the calculated correlation coefficients for the MOSFET and NCFET-designed 4-bit S-box for the PRESENT-80. The correlation coefficients for all potential keys have been displayed, and the dotted line shows the correlation coefficient for the original S-box key ( $K=6$ ). The correlation coefficients of the CMOS Present-80 S-box for all conceivable keys are shown in Fig. 6(a). With the highest correlation for the original key ( $K=6$ ), the DPA attack conducted on the CMOS Present-80 S-box is successful, as can be seen. This suggests that CMOS S-box exhibits more susceptibility to DPA attack by disclosing original key. On the other hand, as depicted in Fig. 6(b), the DPA assault is carried out on the NCFET Present-80 S-box design with  $t_{fe}$  4nm. It is shown that the NCFET PRESENT-80 S-box (4nm) DPA attack fails with the strongest correlation for the wrong key guess. By displaying an incorrect key guess, the NCFET S-box architecture has therefore demonstrated less vulnerability to DPA attack. This is because the increased capacitance of the NCFET device causes the NCFET S-box to display non-linearity in the current traces.

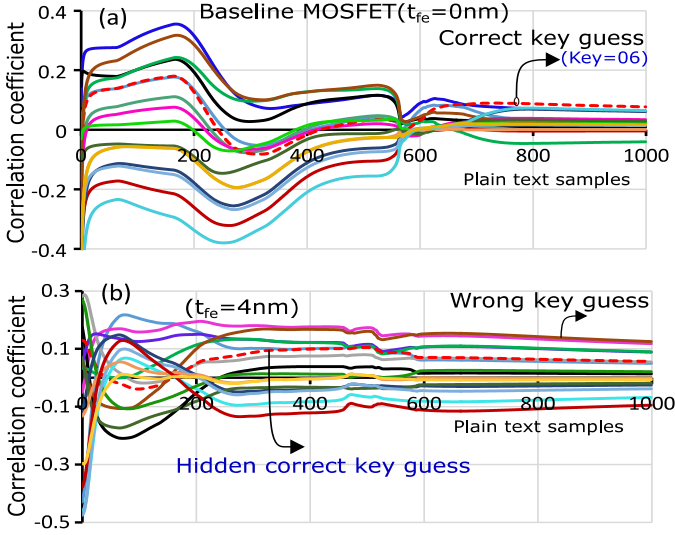


Fig. 6 Correlation coefficient of (a) Baseline 40nm CMOS S-box design (b) NCFET S-box design with  $t_{fe}=4\text{nm}$  at  $V_{DD}=0.5\text{V}$

Thus, NCFET based cipher with  $t_{fe}$  of 4nm is proved to be energy efficient and secure compared to baseline MOSFET based designs.

## Conclusion

This paper for the first time present the design and security evaluation of NCFET based ultra-light weight PRESENT-80 block cipher design at a supply voltage of 0.5V. The NCFET based PRSESNT-80 design is analyzed by varying  $t_{fe}$  of NCFET device. NCFET based PRESENT-80 design at  $t_{fe}$  of 4nm exhibit  $3.2\times$  and  $3.7\times$  lower energy consumption compared to the 40nm baseline CMOS design at 10MHz and 100MHz operating frequencies respectively. Apart from this, the NCFET based PRESENT-80 design is evaluated and proved to be resilient against DPA compared to the baseline MOSFET design by observing power consumption profiles and correlation coefficient. This is due to the non-linear variation of dynamic power consumption profile of NCFET based PRESENT-80 which is obtained from increased input capacitance of NCFET.

## REFERENCES

- [1] L. Tu, X. Wang, J. Wang, X. Meng, and J. Chu, "Ferroelectric negative capacitance field effect transistor," *Advanced Electronic Materials*, Wiley, vol. 4, no. 11, pp.1-17, 2018.
- [2] H. Amrouch, V. M. van Santen, G. Pahwa, Y. Chauhan and J. Henkel, "NCFET to Rescue Technology Scaling: Opportunities and Challenges," 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 637-644, 2020.
- [3] S. Kim, K. Lee, J. -H. Lee, B. -G. Park and D. Kwon, "Gate-First Negative Capacitance Field-Effect Transistor With Self-Aligned Nickel-Silicide Source and Drain," in *IEEE Transactions on Electron Devices*, vol. 68, no. 9, pp. 4754-4757, Sept. 2021.
- [4] O. Prakash, et al., "Impact of NBTI Aging on Self-Heating in Nanowire FET," In *Proc. Design, Automation & Test in Europe Conference & Exhibition*, pp. 1514-1519, 2020.
- [5] R. C. Bheemana, A. Japa, S. Yellampalli and R. Vaddi, "Steep Switching NCFET based Logic for Future Energy Efficient Electronics," 2021 IEEE International Symposium on Smart Electronic Systems (iSES), pp. 327-330, 2021.
- [6] Saeidi, A., Rosca, T., Memisevic, E., Stolichnov, I., Cavalieri, M., Wernersson, L.E. and Ionescu, "Nanowire tunnel FET with simultaneously reduced subthreshold swing and off-current due to negative capacitance and voltage pinning effect," *Nano letters*, vol. 20, no. 5, pp.3255-3262, 2020.
- [7] R. A. Vega, T. Ando and T. M. Philip, "Junction Design and Complementary Capacitance Matching for NCFET CMOS Logic," in *IEEE Journal of the Electron Devices Society*, vol. 9, pp. 691-703, 2021.
- [8] A. Saeidi, F. Jazaeri, I. Stolichnov and A. M. Ionescu, "Double-Gate Negative-Capacitance MOSFET With PZT Gate-Stack on Ultra Thin Body SOI: An Experimentally Calibrated Simulation Study of Device Performance," in *IEEE Transactions on Electron Devices*, vol. 63, no. 12, pp. 4678-4684, Dec. 2016.
- [9] W. You, P. Su and C. Hu, "Evaluation of NC-FinFET Based Subsystem-Level Logic Circuits," in *IEEE Transactions on Electron Devices*, vol. 66, no. 4, pp. 2004-2009, April 2019.
- [10] X. Li et al., "Enabling Energy-Efficient Nonvolatile Computing With Negative Capacitance FET," *IEEE Transactions on Electron Devices*, vol. 64, no. 8, pp. 3452-3458, Aug. 2017.
- [11] S. Salamin et al., "Power-Efficient Heterogeneous Many-Core Design With NCFET Technology," in *IEEE Transactions on Computers*, vol. 70, no. 9, pp. 1484-1497, 1 Sept. 2021.
- [12] N. Chauhan, N. Bagga, S. Banchhor, A. Datta, S. Dasgupta and A. Bulusu, "Negative-to-Positive Differential Resistance Transition in Ferroelectric FET: Physical Insight and Utilization in Analog Circuits," in *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 69, no. 1, pp. 430-437, Jan. 2022.
- [13] Y. Liang, Z. Zhu, X. Li, S. K. Gupta, S. Datta and V. Narayanan, "Utilization of Negative-Capacitance FETs to Boost Analog Circuit Performances," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2855-2860, Dec. 2019.
- [14] R. C. Bheemana, A. Japa, S. Yellampalli and R. Vaddi, "Negative Capacitance FET based Energy Efficient and DPA Attack Resilient Ultra-Light Weight Block Cipher Design," *Microelectronics Journal*, vol. 133, pp.105711, Jan 2023.
- [15] C. -H. Lee, Y. -T. Hsu, T. -T. Liu and T. -D. Chiueh, "Design of an 45nm NCFET Based Compute-in-SRAM for Energy-Efficient Machine Learning Applications," in *Proc. IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 193-196, 2020.
- [16] C. H. Lee, et al., "Design of 45nm NCFET Based Compute-in-SRAM for Energy-Efficient Machine Learning Applications," In *Proc. IEEE Asia Pacific Conference on Circuits and Systems*, pp. 193-196, 2020.
- [17] Japa A, Majumder MK, Sahoo SK, Vaddi R, " Low area overhead DPA countermeasure exploiting tunnel transistor-based random number generator," in *IET Circuits, Devices & Systems*, vol. 14, no. 5, pp. 640-647, Aug. 2020.
- [18] A. Japa, M. K. Majumder, S. K. Sahoo, R. Vaddi and B. K. Kaushik, "Hardware Security Exploiting Post-CMOS Devices: Fundamental Device Characteristics, State-of-the-Art Countermeasures, Challenges and Roadmap," in *IEEE Circuits and Systems Magazine*, vol. 21, no. 3, pp. 4-30, thirdquarter 2021
- [19] R. C. Bheemana, A. Japa, S. Yellampalli and R. Vaddi, "Negative capacitance FETs for energy efficient and

- hardware secure logic designs," in *Microelectronics Journal*, vol. 119, no. 1, pp. 105320, Jan. 2022.
- [20] A. Japa, S.K. Sahoo, R. Vaddi, M.K. Majumder, Emerging tunnel FET and spintronics-based hardware-secure circuit design with ultra-low energy consumption, *J. Comput. Electron* 2022.
  - [21] A. I. Khan, U. Radhakrishna, K. Chatterjee, S. Salahuddin and D. A. Antoniadis, "Negative Capacitance Behavior in a Leaky Ferroelectric," in *IEEE Transactions on Electron Devices*, vol. 63, no. 11, pp. 4416-4422, Nov. 2016.
  - [22] U. Radhakrishna, A. Khan, S. Salahuddin, D. Antoniadis, and U. Berkeley, "Compact model of negative capacitance mosfets (NCFETs)", 2017. [online]. Available: <https://nanohub.org/projects/mvsnctfet>
  - [23] G. Sravya, M. O. V. P. Kumar, Y. Sudarsana Reddy, K. Jamal and K. Mannem, "The Ideal Block Ciphers - Correlation of AES and PRESENT in Cryptography," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020.
  - [24] S. D. Kumar and H. Thapliyal, "Exploration of Non-Volatile MTJ/CMOS Circuits for DPA-Resistant Embedded Hardware," in *IEEE Transactions on Magnetism*, vol. 55, no. 12, pp. 1-8, Dec. 2019.