www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Design of energy-efficient IOT devices using Finfet based secure adiabatic logic

T.M.Sathish Kumar[1], R.Saraswathi[2], S.Ragavi[2]

[1]Assistant Professor, Department of ECE

[2]PG Scholar, Department of ECE, K.S.R. College of Engineering, Tiruchengode-637215.

ABSTRACT

Design of Internet of Things (IoT) is an emerging technique this is widely used to design energy-efficient and secure IoT devices. For example, IoT devices such as Radio Frequency Identification (RFID) tags and Wireless Sensor network Nodes (WSN) employ AES cryptographic module that are vulnerable to Differential Power Analysis (DPA) attacks. As the technology scaled down, leakage power in the cryptographic device increases, which increases their vulnerability to DPA attack but occupation of the device area minimized by the use of FinFET technology. This paper presents a novel FinFET based Secure Adiabatic Logic (FinSAL) that is energy-efficient and has more DPA-immunity. The proposed adiabatic FinSAL is used to construct that logic gates such as buffers, XOR, and NAND. Hence the logic gates based on adiabatic FinSAL are used to design a Positive Polarity Reed Muller (PPRM) architecture based S-box circuit. Then the designed circuit has been simulated with SPICE simulations at 12 MHz and it will reflects that adiabatic FinSAL (20nm FinFET technology) S-box circuit saves power up to 85% of energy per cycle as compared to the conventional S-box circuit implemented using FinFET (20nm FinFET technology). We proved that the FinSAL S-box circuit is highly resistant to a DPA attack through a developed DPA attack flow applicable to SPICE simulations. Further, the impacts of FinSAL on hardware security at different technology nodes of FinFETs (7nm, 10nm, 14nm, 16nm) are evaluated. From the simulation results, FinSAL gates at 14nm FinFET offer superior security with optimum power consumption, therefore is the best candidate to design low-power secure IoT devices.

Keywords: Differential Power Analysis (DPA), ECRL, 2N2N2P, PFAL, FinFETs, hardware security, low-power, adiabatic logic, FinSAL, IoT device S-box circuit.

INTRODUCTION

The quality of life of individuals and societies would improve with the emergence of Internet of Things (IoT).IoT has widespread applications in the field of manufacturing, Automotive, medical, communication, finance etc. [3]. IoT based devices such as Radio Frequency Identification (RFID)tags and Wireless Sensor Nodes (WSN) are used to store and communicate the secret or personal data over the

Internet [4], [5].However, the secret or personal information stored and communicated through these IoT based devices can be obtained through the side-channel attacks [6]. Among the various side-channel attacks reported in the literature, Differential Power Analysis (DPA) attack is considered to be one of the powerful side-channel attacks to reveal the secret information from the secure devices [7]. Various hardware related DPA countermeasures have been developed over the years [8]. But none of these countermeasures are suitable to implement in devices where there is a constraint on power consumption, [9].Adiabatic logic [10] is one of the circuit design techniques to design energy-efficient and secure hardware.

Author for correspondence:
Department of ECE, K.S.R. College of Engineering, Tiruchengode-637215.

Adiabatic logic is also used to design energy-efficient Physical Uncountable Function (PUF) [11]. A survey on DPA countermeasures has concluded that adiabatic logic is one of the promising techniques to design low-power and secure hardware [8]. Further, the usefulness of adiabatic logic circuits for low-power and DPA resistant IoT devices is also established in a recent research article on "Ultralow power and the New era of Not-So-VLSI" [12].With the emergence of IoT, there is an urgent need to design low-power and secure IoT devices. Improvement in the security of these devices comes at the cost of reduction in battery life. Battery life is considered as an important parameter in the design of self-powered IoT devices. Adiabatic logic is considered to be an alternate way to design low-power and DPA-resistant hardware. One of the main features of adiabatic logic is that it can operate efficiently at a frequency less than 1 GHz. Thus, adiabatic logic can be used to design low-power and secure IoT based devices which operate at low frequencies. For example, RFID operates at 13.56 MHz which is in the range where adiabatic circuits can operate energy efficiently.

EXISTING TECHNIQUES

Adiabatic Logic

Adiabatic logic is a design methodology for reversible logic in CMOS where the current flow through the circuit is controlled such that the energy dissipation due to switching and capacitor dissipation is minimized. Adiabatic logic uses power clocks to efficiently recycle the charge stored in the load capacitor. Because of recycling of charge, adiabatic logic has reduced dynamic switching energy loss [2], Fig. 1 shows the adiabatic charging/discharging of the load capacitors.

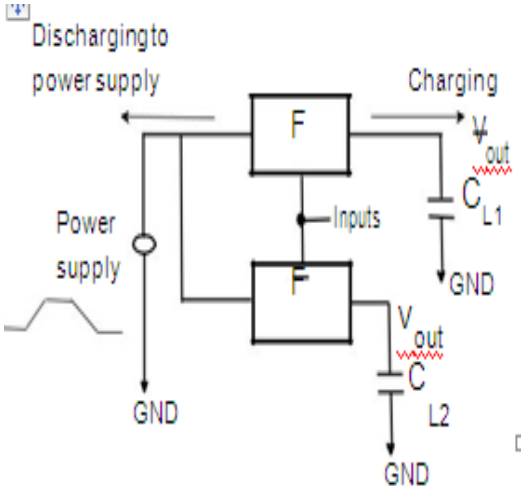

Fig: 1 Structure of Adiabatic Logic

The energy dissipated in an adiabatic circuit when considering the charge is supplied through a constant current source is shown by,

ECRL

The Structure of ECRL illustrated in Fig 2.The ECRL is the one of the technique for adiabatic logic .it has two cross coupled PMOS transistor as a latching elements. These two transistors named as m1 and m2.then the input has been applied to the n tree and the tree is connected with ground.

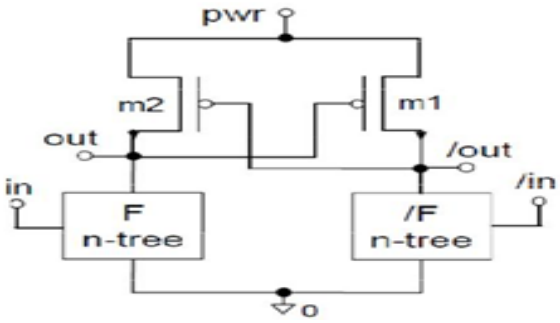

Fig: 2 Structure of ECRL

2N2N2P

The Structure of 2N2N2P illustrated in Fig.3.The 2N2N2P is the one of the technique for adiabatic logic. it has two cross coupled PMOS transistor and two cross coupled NMOS transistor as a latching elements.

PFAL

The Structure of PFAL illustrated in Fig.4. The PFAL is another technique for adiabatic logic. It has two cross coupled PMOS transistor and two cross coupled NMOS transistor as latching elements. It has a latch element formed by two cross-coupled inverters to store the output. Where two n-trees are used to describes the logic functions. This technique used to generates both positive and negative output [13-15].

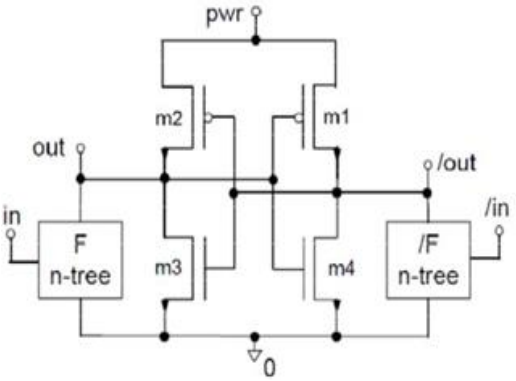

Fig: 3 Structure of 2N2N2P

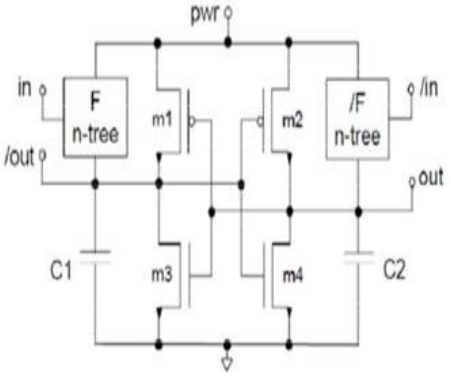

Fig: 4 Structure of PFAL

PROPOSED TECHNIQUE

*FinFETs*Structure

FinFET has a three dimensional structure which has a thin silicon body perpendicular to the plane of the wafer. The channel of the FinFETs is wrapped by the gate in all three directions. Then three dimensional structures of the FinFETs device show in Fig.5. FinFETs offers strong gate control over channels. Strong gate control over channels reduces the short-channel effects, long channel effects threshold current, and gate-dielectric leakage current than MOSFETs. Better gate control in FinFETs s over MOSFETs results in higher on-state current, lower leakage, and faster switching speed. Multi-gate structure of FinFETs allows for different working modes of FinFETs. There are two main working modes for FinFETs are

Shorted-Gate (SG) mode

In the SG mode, double gate (back gate and front gate) of the FinFET are tied together. FinFET acts as a three terminal device in SG mode. Fig. 6a shows the symbol of SG FinFETs

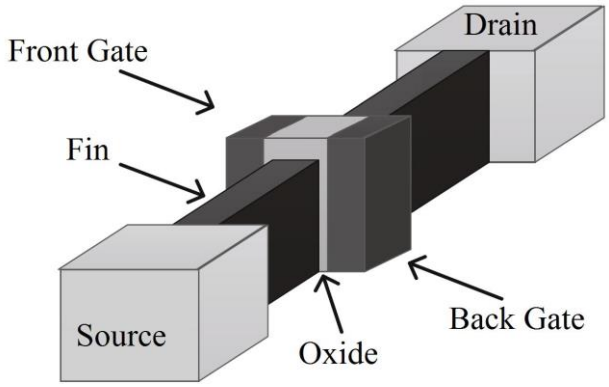

Fig: 5 Structure of FinFET

Independent-Gate (IG) mode

In the IG mode, top part of the gate is removed to form two independent gates. The front gate and back gate are connected to two different inputs. FinFET acts as a four terminal device in IG mode. The special case of IG mode to reduce the threshold leakage is called as Low-Power (LP) mode. Fig. 6b shows the symbol of IG FinFETs

PROPOSED FINFET BASED SECURE

Adiabatic Logic (FINSAL)

The proposed novel logic structure is illustrated in Fig .7 and Structure Analysis of proposed FinSAL xor gateis shown in Fig.8.The working principal of FinSAL has a four phase of operation such as, Wait phase, Evaluate phase, Hold phase, and Recovery phase.

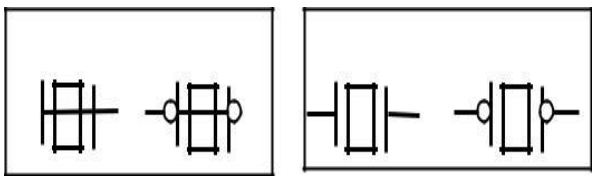

Fig: 6 a) Structure Shorted-Gate (SG) Mode; b) Independent-Gate (IG) Mode

WORKING PRINCIPLE

1).T1 (WAIT PHASE): In this phase, the system power clock VCLK is stable at GND (logic low level). The evaluation path signal is established by M3 or M4 shown in Fig. 8. In this case Fig. 9. Shows that signal slowly rises from 0 to V_{dd} which leads transistor M3 to turn ON.

During the discharge phase the signal high (V_{dd}) this leads to discharging the load capacitances through M5 or M6. The redundant charge stored in load capacitances is discharged to GND before the logic function is evaluated. The evaluation of logic function prevents the circuit from depending on previous input data before discharging the load capacitors occurs.

2).T2 (EVALUATE PHASE): In this phase, DISCHARGE signal is stable at GND (logic low level) which makes OFF M5 or M6. The system power clock slowly rises from low to high level (i.e.) 0 to V_{dd} which leads to current flow occurs at evaluate transistors (M3 or M4). In this case Fig.9 when VCLK rises from 0 to V_{dd}, and the current flow through M3 which leads to the output load capacitor (OUT) to be charged.

3).T3 (HOLD PHASE): During the hold phase, the current active input signal is slowly decrease to 0 levels (GND). The system power clock VCLK is stable at high level (V_{dd}). Then output signal also remains stable in this phase. In this case Fig. 9 shows that signal a slowly decreases from V_{dd} to 0.

4).T4 (RECOVERY PHASE): During the recovery phase, the power clock VCLK slowly reduced from V_{dd} to 0. The current active output discharges to a low level through M1 or M2. The charge stored in the active output load capacitor is discharged to VCLK through M1 or M2. Consequently, charge recovery happens in every clock cycle (T1-T4). Recovering the charge in every clock cycle minimizes the energy lost. In this case Fig. 9 charge stored in the output load capacitor (OUT) is recovered back to VCLK through transistor M1.

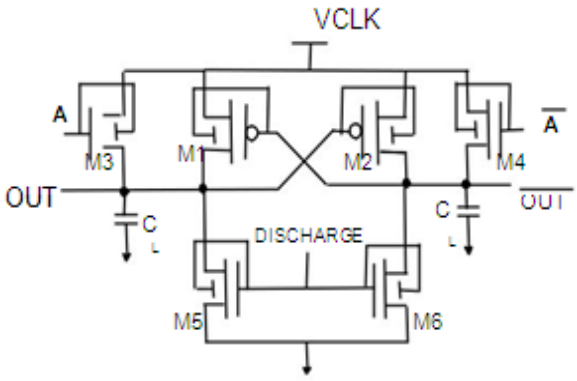

Fig: 7 Structure Analysis of proposed FinSAL

SIMULATION ANALYSIS

The simulated timing analysis of FinSAL output is illustrated in Fig 9. Which has four phase of operation such as T1, T2, T3, T4 and system power clock VCLK, two input A, A bar, output of FinSAL .According to the applied inputs corresponding output has been varied. Simulated analysis of signal to noise ratio vs. No of input of FinSAL illustrated in Fig 10.Then the FinFETs are categorized as different technology such as 7nm, 10nmm, 14nm, 16nm, 20nm. Similarly Simulated analysis of signal to noise ratio vs. frequency of FinSAL illustrated in Fig 11 .Then the FinFETs are categorized as different technology such as 7nm, 10nmm, 14nm, 16nm, 20nm.

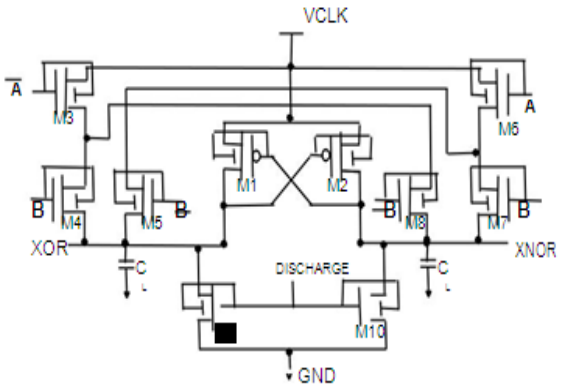

Fig:8 Structure Analysis of proposed FinSAL xor gate

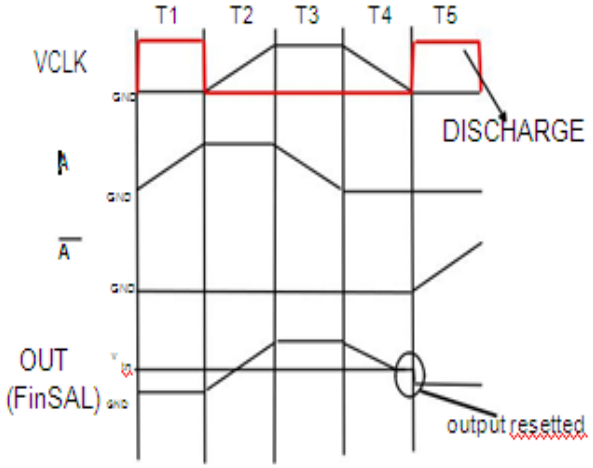

Fig: 9Timing Analysis of FinSAL

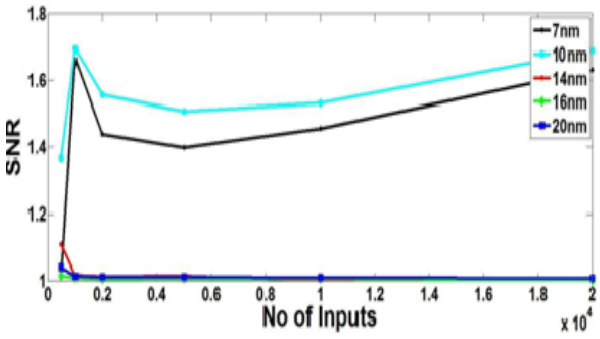

Fig: 10 Analysis SNR vs. No of input of FinSAL

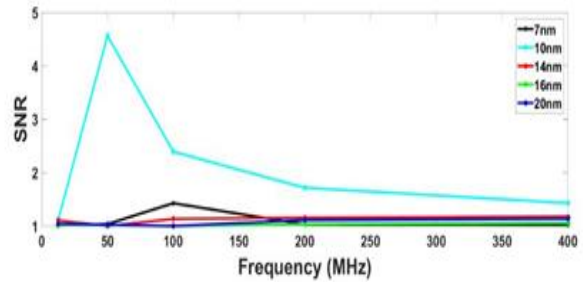

Fig: 11 Analysis SNR vs. frequency of FinSAL

The current consumption of conventional FinSAL and current consumption of proposed FinSAL illustrated in Fig 12 and Fig 13(a), (b).Then graph has been plotted between currentvs. time and Fig. 14 shows the energy consumed during each period of the adiabatic FinSAL and FinFET based conventional xor gate. The graph has been plotted between energy vs time. The FinFET based conventional logic suffers from dynamic power dissipation whenever there is an input transition occurs. In the proposed adiabatic FinSAL logic, there is a less non-adiabatic energy loss during the reset of outputs. But the proposed adiabatic FinSAL logic consumes less energy as compared to the FinFET based conventional logic.

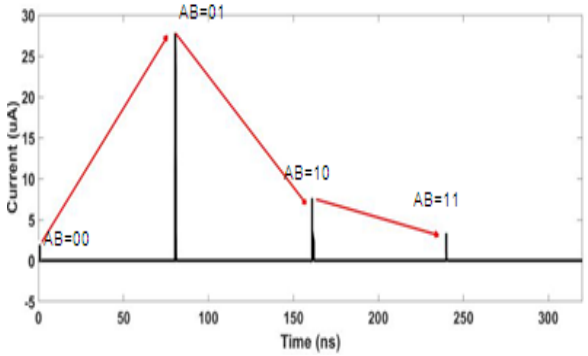

Fig: 12 Current Consumption of conventional FinFET

The current consumption of FinFET based xor gate is not uniform due to that enormous amount power has been dissipated .but the proposed FinSAL based xor gate is uniform then problems of the power dissipation has been removed by equally sized FinFET transistor. The FinFET technology has more intrinsic capacitance the MOSFET technology.

CONCLUSION

The proposed design of energy efficient IOT devices using FinFET based adiabatic logic have been designed and simulated using the cadences tools. This one of the dynamic power resistant logic called as FinSAL. Signal to noise ratio vs. no of input and signal to noise ratio vs. frequency has been analyzed with various FinFET technology such as 7nm,10nm,14nm,16nm,20nm. Then compared with the different FinFET technology 14nm technology has provides higher security then the other technology. The FinSAL has more power resistant, high security, low power consumption, FinSAL is mostly suitable for portable electronics devices.

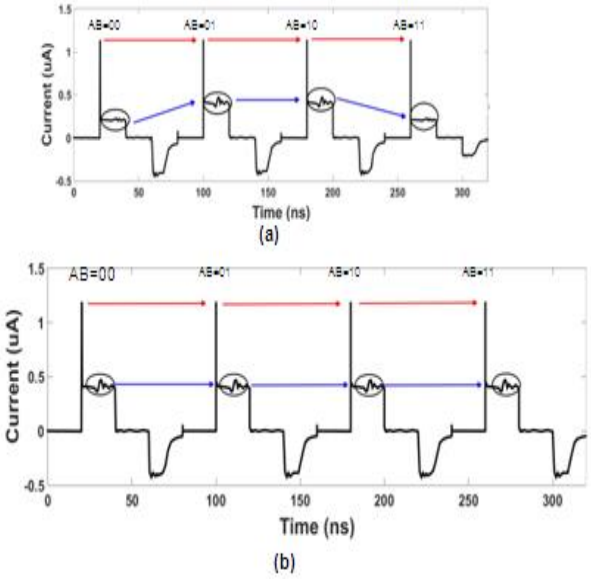

Fig: 13 Current consumption of proposed FinSAL
(a) FinFETs are equally sized
(b) Effective width of FinFETs

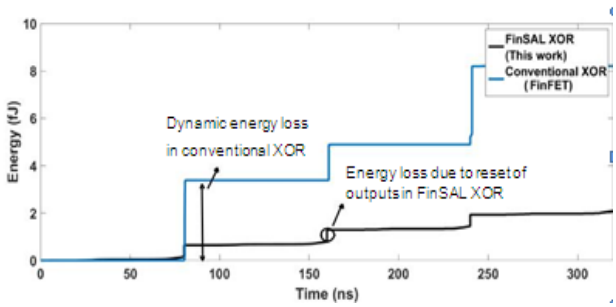

Fig: 14 Energy consumption of proposed FinSAL vs. conventional

REFERENCES

[1]. S. D. Kumar, H. Thapliyal, A. Mohammad, V. Singh, and S. K. Perumalla, "Energy-efficient and secure s-box circuit using symmetric pass gate adiabatic logic," in Proceedings of the IEEE computer society Annual Symposium on VLSI (ISVLSI). IEEE, 2016.

[2]. D. Kumar, H. Thapliyal, and A. Mohammad, "Finsal: A novel finfet based secure adiabatic logic for energy-efficient and dpa resistant iot devices," in IEEE International Conference on Rebooting Computing. IEEE, 2016.

[3]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[4]. E. Ilie-Zudor, Z. Kemeny,´ F. van Blommestein, L. Monostori, and A. van der Meulen, "A survey of applications and requirements of unique identification systems and rfid techniques," Computers in Industry, vol. 62, no. 3, pp. 227–252, 2011

[5]. W. Cheng, S. Wang, and X. Cheng, "Virtual track: applications and challenges of the rfid system on roads," IEEE Network, vol. 28, no. 1, pp. 42–47, 2014.
[6]. D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Com-munications, vol. 58, no. 1, pp. 49–69, 2011.
[7]. P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," Journal of Cryptographic Engineering, vol. 1, no. 1, pp. 5–27, 2011.
[8]. A. Moradi and A. Poschmann, "Lightweight cryptography and dpa coun-termeasures: A survey," in Financial Cryptography and Data Security. Springer, 2010, pp. 68–79.
[9]. M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish,"Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes," Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 62, no. 1, pp. 149–156, 2015.
[10]. W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Y.-C. Chou, "Low-power digital systems based on adiabatic-switching princi-ples," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 2, no. 4, pp. 398–407, 1994.
[11]. S. D. Kumar and H. Thapliyal, "Qualpuf: A novel quasi-adiabatic logic based physical unclonable function," in Proceedings of the 11th Annual Cyber and Information Security Research Conference. ACM, 2016,p.24.
[12]. M. Wolf, "Ultralow power and the new era of not-so-vlsi," IEEE Design & Test, vol. 33, no. 4, pp. 109–113, 2016.
[13]. M. Khatir and A. Moradi, "Secure adiabatic logic: a low-energy dpa-resistant logic style." IACR Cryptology ePrint Archive, vol. 2008, p. 123, 2008.
[14]. B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric adi-abatic logic circuits against differential power analysis," ETRI journal, vol. 32, no. 1, pp. 166–168, 2010
[15]. C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level," Microelectronics Journal, vol. 44, no. 6, pp. 496–503, 2013.