ENGINEERING IN ADVANCED RESEARCHSCIENCE AND TECHNOLOGY

ISSN 2352-8648
Vol.04, Issue.02
December-2021
Pages: -599-609

POWER AND DENSITY OPTIMIZED SYMMETRIC PASS GATE USING GDI

[1]BUSI SUDHAKARA RAO, [2]A.NAGA SUMAN

[1]PG Student, Dept. of ECE, VKR, VNB &AGK college of Engineering , Gudivada, A.P

[2]Associate professor, Dept. of ECE, VKR, VNB &AGK college of Engineering , Gudivada, A.P

ABSTRACT: Internet of Things (IoT) devices have strict energy constraints as they often operate on a battery supply. The cryptographic operations within IoT devices consume substantial energy and are vulnerable to a class of hardware attacks known as side-channel attacks. In this paper, we propose 2-SPGAL, a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). Aagain look to adiabatic logic to design secure circuits with uniform power consumption, thus, defending against power analysis attacks. Further, this project is enhanced by using gate diffusing input to further reduce both area and power constraints as an optimization of proposed method.

Keywords: Adiabatic Logic, Symmetric Pass Gate, cryptographic, Internet of Things, Correlation Power Analysis Attacks.

INTRODUCTION: Internet of Things (IoT) devices are necessary for the functions of modern life. IoT devices have a wide range of uses from the manufacturing sector [1] to everyday consumer products [2]. Many of these IoT devices are battery operated and thus reduced energy consumption is key to extending the use of these devices. Furthermore, many of these IoT devices, such as medical devices, transmit and store sensitive data thus making them prime targets for hardware attacks [3]. Flying ad hoc networks must be energy-efficient to remain mobile and functioning for long periods of time [4]. Further, the communication testbeds for these networks are a potential point for hardware attacks. One form of hardware attack IoT devices face is a side-channel attack. Side-channel attacks look to exploit secure information through a device's side channels such as power consumption [5], timing [6], etc. Defense mechanisms against side-channel attacks can cause drastic energy increases; thus, the ideal solution should reduce energy consumption while defending against side-channel attacks [7,8]. Novel design techniques such as adiabatic logic are promising to both reduce energy consumption and defend against a type of side-channel attack known as power analysis attacks [9]. Adiabatic logic reduces the dynamic energy consumption of a circuit by recycling stored charge in the load capacitor back into the clock to be used again [10]. Furthermore, dual-rail adiabatic circuits can be designed so that the circuits are balanced and power consumption remains uniform preventing information leakage [9]. Figure 1 shows the categories of countermeasures against Correlation Power Analysis Attacks (CPA). Adiabatic logic is an emerging design technique for designing low-energy circuits [10]. Adiabatic logic lowers energy consumption by recycling current stored within an adiabatic circuit's load capacitor back into the clock. An adiabatic clock generator uses capacitors and inductors as storage elements for the recovered energy. The recovered energy is then reused in the next clock cycle thus reducing the energy of the circuit. With this information, an attacker can measure hundreds of thousands of power profiles with controlled inputs to steal the secure encryption key. Masking and elimination are two methods to defend against power analysis attacks [22]. Masking aims to minimize correlation between data and power consumption such as in the proposed Bus-Invert Coding [3]. To defend against the CPA attack, we designed our circuits using a technique known as elimination [2]. Elimination aims to remove any variations in power consumption, so that each operation has uniform power consumption and thus no information leakage.

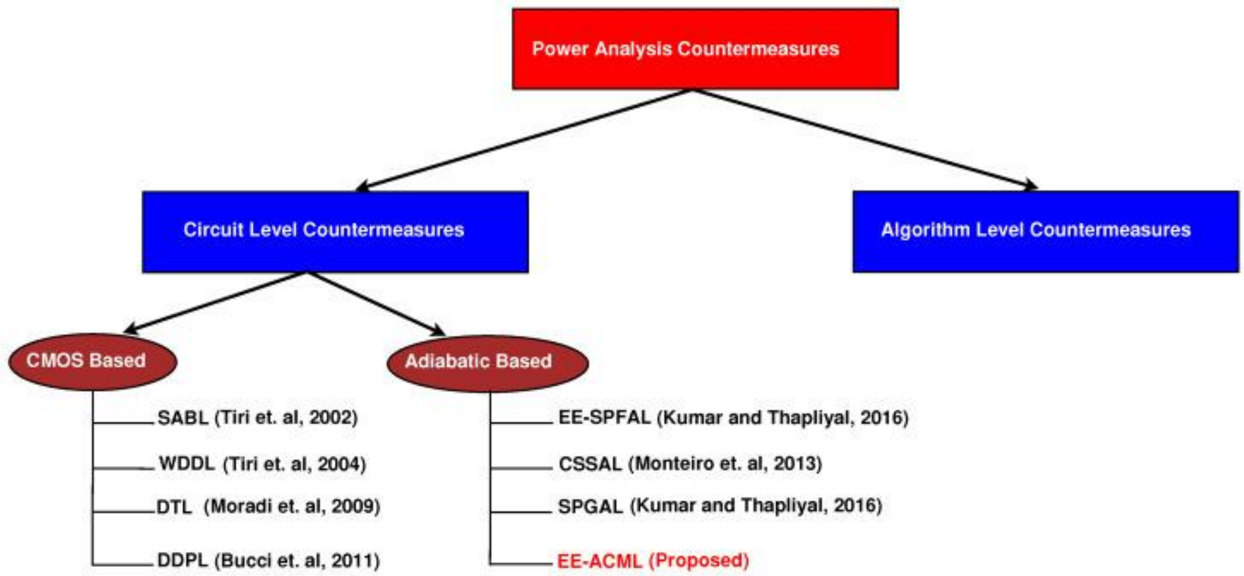


Figure 1 Correlation Power Analysis Countermeasures

Along with adiabatic logic, novel devices such as Magnetic Tunnel Junctions (MTJs) can also be used to design low energy and secure circuits [15]. MTJs are nonvolatile storage units that have low standby power, high integration density, and easy compatibility with CMOS [16,17,18]. MTJs can be added to CMOS structures to form nonvolatile ultra-low energy circuits [9]. In this article, we propose a novel hybrid adiabatic CMOS/MTJ logic named Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML). To demonstrate energy savings of EE-ACML integrated with an adiabatic clock generator, we designed one round of PRESENT. PRESENT is a lightweight encryption algorithm making it an ideal candidate for IoT devices. In our EE-ACML implementation of PRESENT, we showed that our circuit had energy savings of 67.24% at 25 MHz and 86.5% at 100 MHz when compared with a previously proposed CMOS/MTJ circuit. We have also shown that our proposed EE-ACML PRESENT implementation remains secure with the adiabatic clock generator implemented by performing a Correlation Power Analysis Attack (CPA) and determining the key was not revealed. A preliminary version of this paper appeared in [2].

LITERATURE SURVEY: Dynamic logic families achieve low energy dissipation but it uses multiple phase clocks to control cascaded gates. It cannot be used for high speed design instead of clock skew management problems. True single phase energy recovering logic circuit uses single phase clock scheme. Energy recovery will be in terms of energy efficiency and operating speed. TSEL address dissipates half of the power at 280MHz. In adiabatic logic, when input is high, half of the input is given to PMOS transistors equivalent resistor and another half of the input is given to the load capacitor. When input is low, then another half stored in the capacitance will be given to PMOS transistor-resistor. The 2N-2N2D adiabatic logic uses diodes. The diode will generate lower bound of energy. In 2N-2P, 2N-2N2P does not have any diodes and it uses four phase clocks for controlling cascading gates, but it will produce non-adiabatic switching event occurs during the longer interval in the evaluation phase.CAL circuits achieve half the throughput of 2N-2NAP circuits [8]. Adiabatic logic uses digital circuit design for reducing power. Adiabatic logic is used to design fundamental logic gates such as NOT, NAND, NOR and XOR which will generate improved power dissipation than static CMOS logic style. The simulation results were carried out by using NImultisim software with 0.18μm, 1.8V CMOS standard process technology for frequency ranges between (200- 800) MHz. Conventional static CMOS logic uses DC power supply and it can be replaced by trapezoidal/ sinusoidal power source to reduce adiabatic energy loss. Transition time is inversely proportional to energy loss. When the time interval between signals is equal, the voltage drop is less so, power dissipation will be lower. In evaluate phase, the outputs are evaluated corresponding to the input state, during the hold state, the output is maintained and applied to the cascaded circuit. In recover phase, the energy is recovered and given back to the power source. Finally wait state is used for avoiding asymmetry.

EXISTING TECHNIQUE: Adiabatic logic is based on charging capacitive load using constant current rather than usual constant voltage [6]. However, designing the constant current source is a challenging task, thus in practice, a ramp voltage source is preferred as a replacement for constant current voltage. The ramp signal is usually referred to as Power Clock (PC) which serves as a power and clock source in an adiabatic circuit. As shown in Figure 2, the reduction in energy consumption in adiabatic logic is achieved. This is because as the energy stored in the capacitor after the end of each clock cycle is utilized in a successive clock cycle. The amount of energy consumed in adiabatic is given by equation 1.

$$E_{\text{diss}} = \frac{RC}{T} C V_{dd}^{2} \qquad (1)$$

In equation 1, T is the charging or discharging period of the load capacitor C, R is resistance due to transistor, and V dd is the full-swing voltage in PC. We can see that if T is maintained greater than RC then, the energy consumption turns out to be less than standard CMOS.

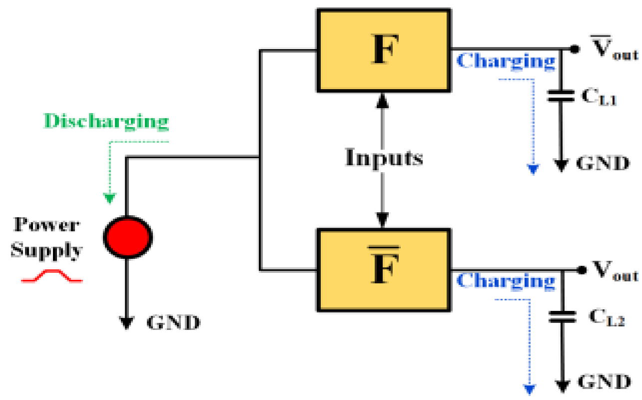


Fig. 2: Charging and discharging in adiabatic circuits

SYMMETRIC PASS GATE ADIABATIC LOGIC:

Symmetric Pass Gate Adiabatic Logic (SPGAL) is a CPA resistant adiabatic logic style [8]. The SPGAL structure, as shown in Figure 3, can be categorized into three blocks, two balanced evaluation blocks: a sense amplifier, and a discharge circuit. SPGAL was originally proposed on a 4-phase clocking scheme [8]. Two pmos transistors M1 and M2, are connected in a back-to-back fashion to construct a sense amplifier/latch. The evaluation network produces the output bit set as per input signal condition at evaluation blocks. The discharge transistor M3 and M4 help to reset the output to maintain uniform power consumption.

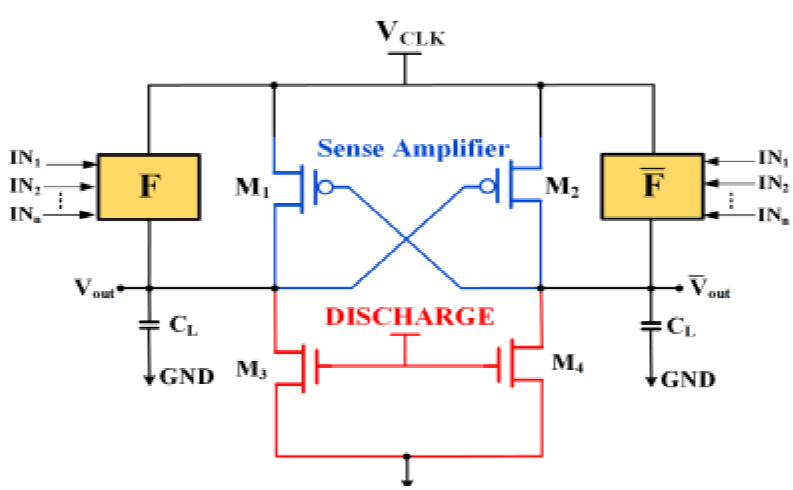


Fig. 3: General SPGAL gate structure [8].

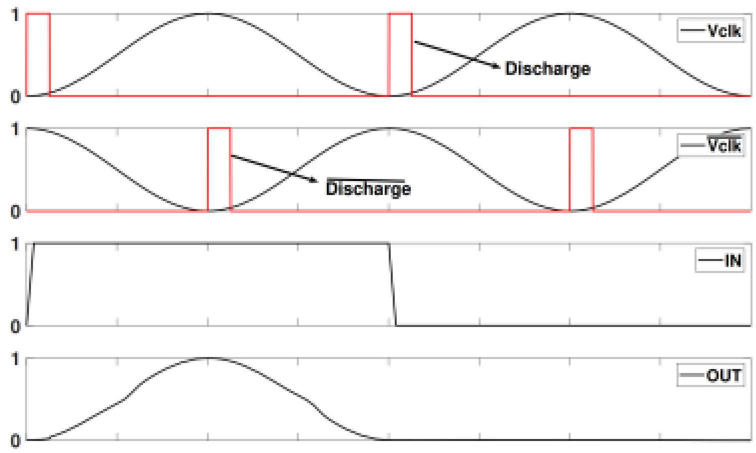


Fig4: Wave analysis

In this paper, we propose 2-SPGAL that is a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). We used two out-ofphase sinusoidal waves (Figure 4) [9]. The rising sinusoidal signal is the ”evaluate” phase and the falling sinusoidal works as the ”recover” phase. Further, there are two discharge signals, in ”synchronization” with their respective clock signal. By the word ”synchronization”, we mean that the time-period and delay of the discharge signals should match with their respective sinusoidal clock signal. The reduced number of the clocks, e.g. 2-phase [11] vs. 4-phase [12] can result in a less complex clock generator design and fewer area requirements.

DRAWBACKS:

1. More power consumption with nor reliability
2. Huge gate density with leakage power
3. More processing time with large combinational path delay

PROPOSED METHOD:

GATE DIFFUSION TECHNIQUE: The GDI method is based on the use of a simple cell as shown in Fig. 1. At a first glance the basic cell resembles the standard CMOS inverter, but there are some important differences: GDI cell contains three inputs – G (the common gate input of the nMOS and pMOS transistors), P (input to the outer diffusion node of the pMOS transistor) and N (input to the outer diffusion node of the nMOS transistor). The Out node (the common diffusion of both transistors) may be used as input or output port, depending on the circuit structure.

The GDI cell is similar to a CMOS inverter structure. In a CMOS inverter the source of the PMOS is connected to VDD and the source of NMOS is grounded. But in a GDI cell this might not necessarily occur. There are some important differences between the two. The three inputs in GDI are namely-

1) G- common inputs to the gate of NMOS and PMOS
2) N- input to the source/drain of NMOS
3) P- input to the source/drain of PMOS

Bulks of both NMOS and PMOS are connected to N or P (respectively), that is it can be arbitrarily biased unlike in CMOS inverter. Moreover, the most important difference between CMOS and GDI is that in GDI N, P and G terminals could be given a supply ‘VDD’ or can be grounded or can be supplied with input signal depending upon the circuit to be designed and hence effectively minimizing the number of transistors used in case of most logic circuits (eg. AND, OR, XOR, MUX, etc). As the allotment of supply and ground to PMOS and NMOS is not fixed in case of GDI, therefore, problem of low voltage swing arises in case of GDI which is a drawback and hence finds difficulty in case of implementation of analog circuits.

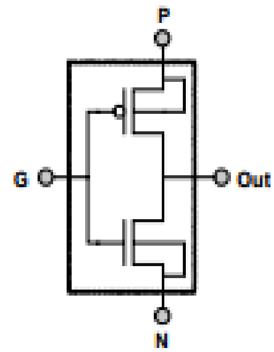


Fig:5 Basic GDI cell

Multiple-input gates can be implemented by combining several GDI cells. The buffering constrains, due to possible VT drop are described in detail in [8], as well as the technological compatibility with CMOS (and with SOI).Morgenshtein has proposed basic GDI cell shown in Fig.1 [8]. This is a new approach for designing low power digital combinational circuit.GDI technique is basically two transistor implementation of complex logic functions which provides in-cell swing restoration under certain operating condition. This approach leads to reduction in power consumption, propagation delay and area of digital circuits is obtained while having low complexity of logic design. An important feature of GDI cell is that the source of the PMOS in a GDI cell is not connected to VDD and the source of theNMOS is not connected to GND. Therefore GDI cell gives two extra input pins for use which makes the GDI design more flexible than CMOS design. There are three inputs in a GDI cell - G (common gateinput of NMOS and PMOS), P (input to the source/drain ofPMOS) and N (input to the source/drain of NMOS).Bulks ofboth NMOS and PMOS are connected to N and Prespectively. Table 1 shows different logic function is implemented by GDI logic [8] based on different input values. So, various logic functions can be implemented with less power and high speed with GDI technique as comparedto conventional CMOS design.

S.No.	N I/P	P I/P	G I/P	Output	Function
1.	0	B	A	A'B	F_1
2.	B	1	A	A'+B	F_2
3.	1	B	A	A+B	OR
4.	B	0	A	AB	AND
5.	C	B	A	A'B+AC	MUX
6.	0	1	A	A'	NOT

LOGIC FUNCTIONS OF BASIC GDI CELL

GDI decreases both gate leakage current and sub threshold leakage current as compared to traditional CMOS. But its performance depreciates when used in and below 90nm technology. Fabrication of basic GDI cell is not possible in traditional p well progression. When substrate attached to drain, threshold voltage is increased and when the substrate is attached to source, body effect is destroyed in below equations

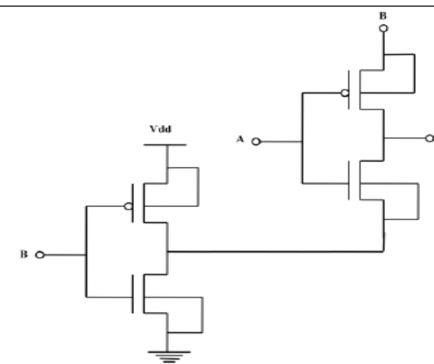
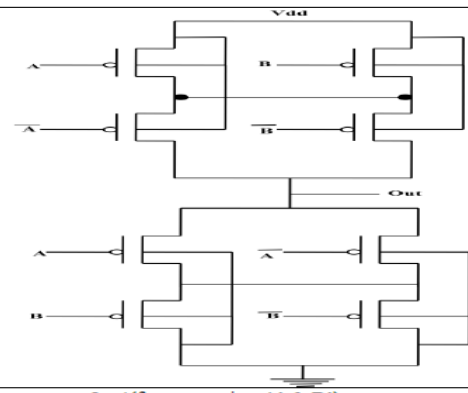
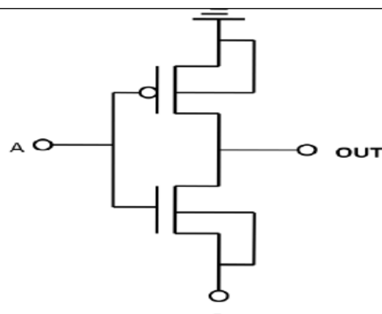
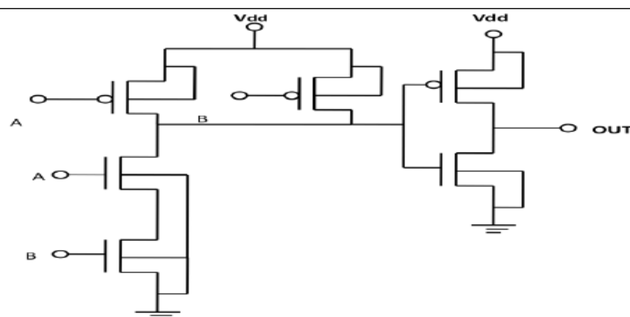
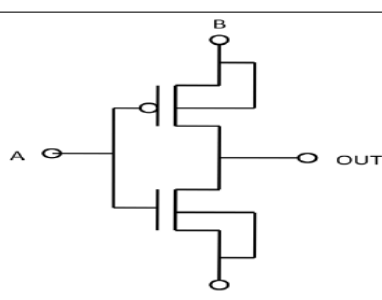
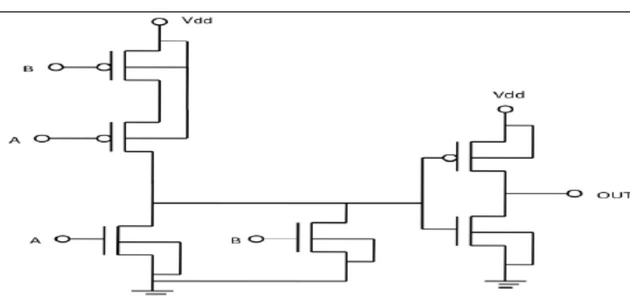
$$V_{th} = V_{tho} + \gamma\left(\sqrt{|\,2\emptyset_F + V_{SB}\,|} - \sqrt{|\,2\emptyset_F\,|}\right) - \eta V_{DS}$$

'Vth' stands for threshold voltage, VSB stands for source body voltage, 'Vtho' stands for zero bias threshold voltage, 'γ' stands for substrate bias coefficient, 'ΦF' is fermi potential, 'VSB' Source to substrate voltage, 'VDS 'drain to source voltage and 'η' is drain induced barrier lowering (DIBL) coefficient

GDI CELL USING SHANNON EXPANSION :

The concept of Shannon theorem could be applied with ease to design a basic GDI cell. In Shannon expansion theorem, any function F can be written as: F(x1…xn) = x1H(x2….xn) + (not x1)G(x2…xn) = x1F(1,x2…xn)+(notx1)F(0,x2….xn) (1) That is a larger function can be broken down into smaller function as shown above in equation (1). Then, the smaller functions could be further broken down if possible till the time it is not further reducible. The output function of a basic GDI cell (where A, B, and C are inputs to G, P, and N, respectively) is given by: Out=AC + (notA) B (2) Therefore, comparing equations (1) and (2) it is seen that a standard GDI cell can be used to implement any logic function based on Shannon expansion theorem as shown below taking an example. If A=x1, C=F(1,x1….xn), B=F(0,x1…..xn) then Out=F(x1…xn)=x1F(1,x2…xn) +(not x1) F(0,x2…xn) (3)

COMPARATIVE STUDY OF GDI AND CMOS SCHEMATICS:

Gate		
XOR		
	Transistor count- 4	Transistor count- 8 +4(for generating A' & B')
AND		
	Transistor count- 2	Transistor count-6
OR		
	Transistor count- 2	Transistor count- 6

The GDI cell has n + 2 inputs when compared to CMOS; Arkadiy Morgenshtein et al. (2002) analyzed the performance of GDI in terms of noise margin, body effect, fan out and delay etc. In realizing the function, F1 = Ɨ.b, it has been found that the behavior of GDI cell is similar to that pMOS pass transistor logic in which the output is at Vtp instead of 0. This is the only case where logic degradation of one Vt takes place. In order to restore the logic, the GDI based buffer is added at the output. The GDI cell can act as a buffer when P=1 which performs its logic evaluation and also restore the logic. This is a main advantage of GDI cell. The GDI cells have less Vt drop in some of the transitions at the output of the cell. With a proper interconnection of the cells, several GDI cells are connected in series or parallel without accumulating the voltage drop. In order to restore the logic swing, an inverter is used at the output (which can also perform its logical function). In this way, the Vt drop and noise margin reductions are localized. However, there are also potential advantages in GDI in terms of reliability. They include these:
x The lower voltage levels have lower impact due to crosstalk on neighboring wires. x The fact that complex functions are built by using multiple instances of the same GDI cell contributes to reduced variability, and x Smaller area and number of transistors in GDI mean shorter interconnects and less crosstalk and these enable more efficient place and route. Various logic functions for different input combinations of GDI cell, which are used in this design are furnished Most of these functions when implemented using CMOS, as well as in regard to standard pass transistor logic implementations are complex (6–12 transistors). But they are very simple (only two transistors per function) in the GDI design method.

RESULTS:

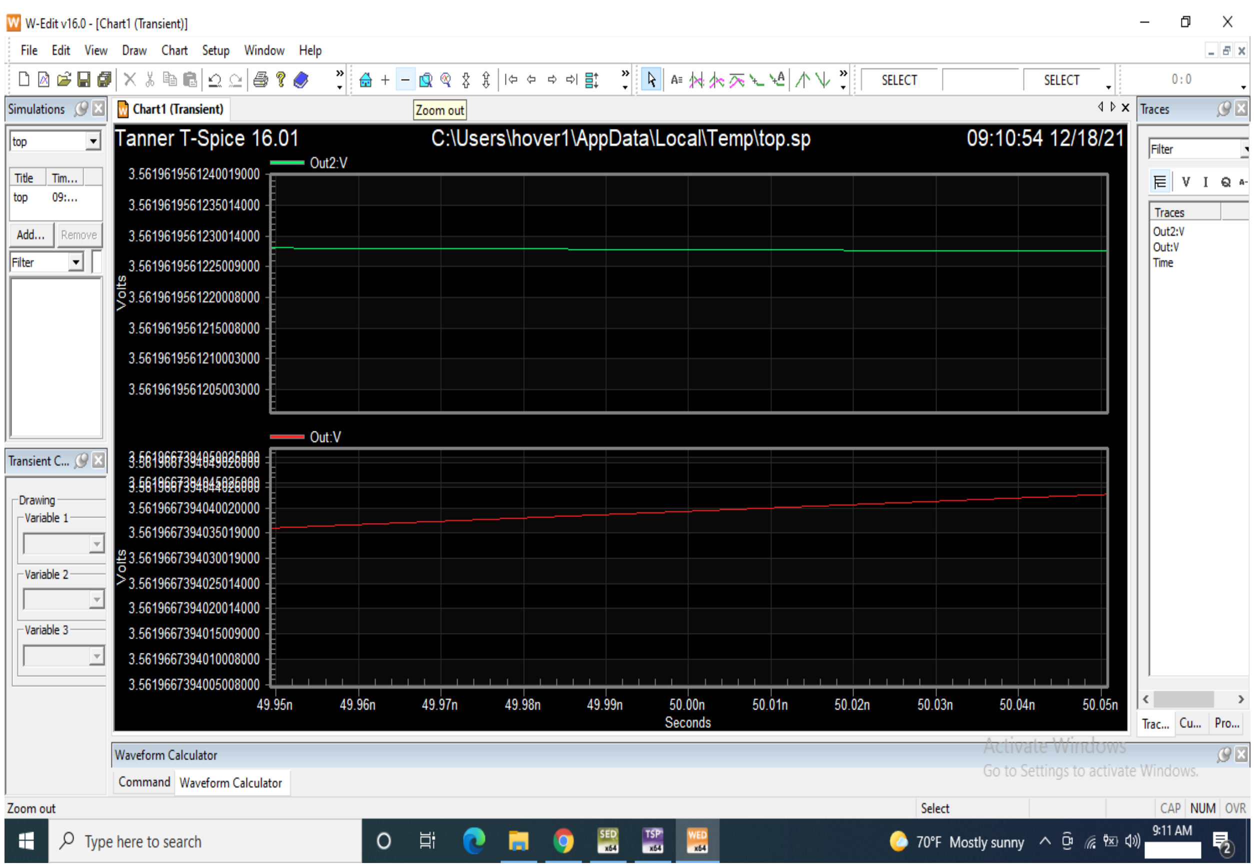


Fig6: Existing simulation result

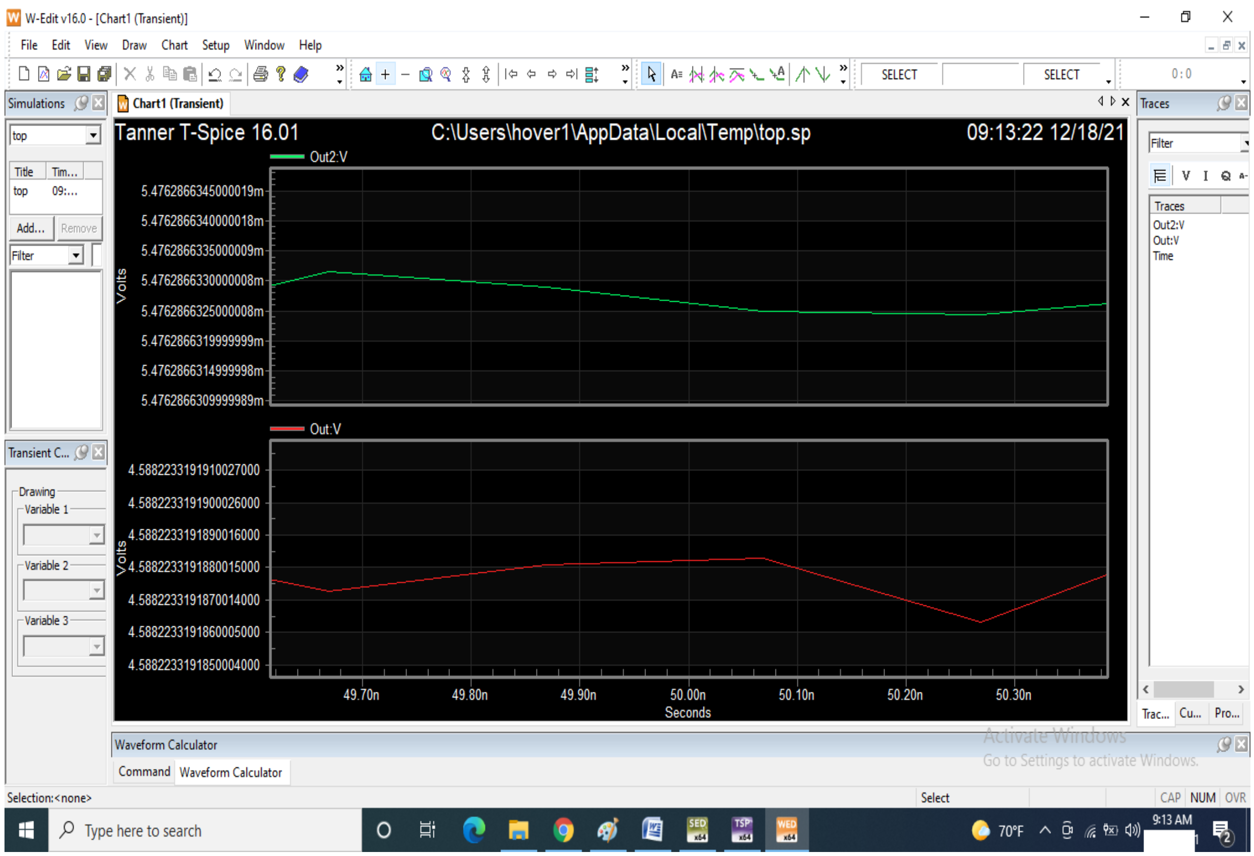


Fig7: Proposed simulation result

ADVANTAGES: The first thermodynamic process theory which we have believe to be applied in the coffee maker is adiabatic process. The reason why we chose this process is because the filter of the coffeemaker is actually made up of adiabatic materials. Advantages of PFAL is transmission gate fromation, positive and negative ouputs generated through the functional blocks.

CONCLUSION: Implemented GDI based 2-SPGAL, a 2-phase sinusoidal signal based clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL), is a new logic style for low-power and secure computing using energy recovery circuits. 2-SPGAL requires few transistors compare to existing work on 2-phase secure adiabatic logic (2-EE-SPFAL). The 2-SPGAL shows significant energy saving at different frequencies compared to 2-EE-SPFAL and standard CMOS. Further, we demonstrated 2-SPGAL based PRESENT-80 is resistant against the CPA side-channel attack as a case study. In the future, post-layout area analysis and its effect on capacitance need to be evaluated. In conclusion, the proposed 2-SPGAL is a promising logic style to design secure and energy-efficient IoT edge computing nodes, Radio Frequency Identification (RFID), and Cyber Physical System (CPS).

FUTURE SCOPE: However, there is 1.4 times increase in delay of design whereas, for MOD 2, there is no change in delay of GDI based technique as compared to those implemented in the standard CMOS technology. Due to no change in delay forMOD 2, the improvement in PDP is 27%, but for MASH 1-1 theimprovement is 15%. The entire work uses audio frequency range,and comparison of the two methods show equal performance parameter measurement values of SNDR, SNR, SFDR, and ENOB. The same idea can be extended to high-resolution modulators and also to higher order digital modulators, where the reduction in area, delay, and PDP can be even greater. References Baker, R. Jacob, 2010. CMOS Circuit Design, Layout, and Simulation.

REFERENCES

[1] Akintunde, M. A., Adegoke, C. O. and Papetu, O.P, "Experimental investigation of the performance of a design model for vapor compression refrigeration systems", West Indian J. Engin., Vol. 28, No. 2, (2006).
[2] Akintunde, M. A., "Effect of coiled capillary tube pitch on vapor compression refrigeration system performance", Au. J.T., vol. 11,no. 1, pp. 14-22, July (2007).
[3] Vaibhav Jain, S. S. Kachhwaha, R. S. Mishra. "Comparative performance study of vapour compression refrigeration system with R22/R134a/R410A/R407C/M20". International Journal of Energy and Environment, Volume 2, Issue 2, pp.297-310, 2011.
[4] Richa Soni*, P.K,Jhinge and R.C.Gupta, "Performance of window air conditioner using alternative refrigerants with different configurations of capillary tube", International journal of current research and academic review, ISSN: 2347-3215 Vol 4 (2013), pp 46-54.
[5] Hirendra Kumar Paliwall, Keshav Kant2 , " A model for helical capillary tubes for refrigeration systems," International Refrigeration and Air Conditioning Conference Purdue University , 2006
[6] M.Y.Taib, A.A.Aziz and A.B.S.Alias, "Performance analysis of a domestic refrigerator", National Conference in Mechanical Engineering Research and Postgraduate Students, 2010.
[7] Sanggoon Park, Kidong Son, Jihwan Jeong and Lyunsu Kim, "Simulation of the effects of a non-adiabatic capillary tube on refrigeration cycle", International Refrigeration and Air Conditioning Conference, 2008.
[8] J.K.Dabas, A.K.Dodeja, Sudhir Kumar and K.S.Kasana, "Performance characteristics of "vapour compression refrigeration system" under real transient conditions", International Journal of Advancements in Technology, 2011.
[9] M.M.Tayde, Pranav Datar and Pankaj Kumar, "Optimum choice of refrigerant for miniature vapour compression refrigeration system", Indian journal of Applied Research, 2013.
[10] Nishant P. Tekade and Dr. U.S.Wankhede, "Selection of spiral capillary tube for refrigeration appliances", International Journal of Modern Engineering Research, 2012.
[11] Ankush Sharma and Jagdev Singh, "Experimental investigation of refrigerant flow rate with spirally coiled adiabatic capillary tube in vapour compression refrigeration cycle using eco friendly refrigerant", International Journal of Mechanical and Production Engineering Research and Development, 2013.
[12] Sudharash Bhargava and Jagdev Singh, "Experimental study of azeotropic blend (30% propane, 55% n-butane, 15% iso-butane) refrigerant flow through the serpentine capillary tube in vapour compression refrigeration system", International Journal of Mechanical and Production Engineering Research and Development, 2013.
[13] Thamir K. Salim, "The effect of the capillary tube coil number on the refrigeration system performance", Tikrit Journal of Engineering Sciences, 2012.
[14] Akash Deep Singh, "Flow characteristics of refrigerant inside diabatic capillary tube," Thapar University, Patiala, (2009), pp. 1-96.
[15] N. Anuar, Y. Takahashi, T. Sekine, "Two-Phase clocked adiabatic static CMOS logic and its logic family" Journal of semiconductor technology and science, vol 10, no. 1, Mar. 2010, pp. 1-10.
[16] M. Saeki, D. Suzuki, and T. Ichikawa, "Leakage analysis of DPA countermeasures at the logic level," lElCE Trans. Fundamentals., vol. E90-A, no. 1, pp. 169-178, Jan. 2007.
[17] M. Alioto and G. Palumbo, "Performance evaluation of adiabatic gates," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 47, no. 9, Sep 2000.
[18] S. Kim, M. C. Papaefthymiou, and C. H. Ziesler, "A true single-phase 8-bit energy-recovery multiplier," IEEE Transactions on VLSI Systems, vol. 11, no. 2, pp. 194–207, Apr 2003.
[19] M. C. Knapp, P. J. Kindlmann, and M. C. Papaefthymiou, "Implementing and evaluating adiabatic arithmetic units," IEEE 1996 Custom Integrated Circuits Conference, pp. 115–118, 1996.