TFET Based DPA Resistant Secured Adiabatic Logics for Energy Efficient and Secure hardware

Vrushali Gandla
Dept. of Electronic & Communication
VIT Chennai
Chennai ,TN, India

Kasthuri Thilagam
Dept. of Electronic & Communication
VIT
Chennai, TN, India

Anil Srikanth
Dept. of Electronic & Communication
IIT
Madras,TN, India

Abstract - **Adiabatic logic is one of the design techniques for designing energy- efficient hardware. Low-power mobile devices such as RFID tags and WSNs that employ cryptographic modules are susceptible to differential power analysis (DPA) attacks. The secret information stored in these hardware devices can be explored by side channel effects. A Secured Quasi-Adiabatic Logic (SQAL) has been proposed in designing Differential Power Analysis (DPA)-resistant and energy-efficient hardware. SQAL shows improvement over all other existing DPA resistant adiabatic logic in terms of energy dissipation and area-overhead. However, the drawback is, SQAL suffers from non-adiabatic energy loss during the evaluation of the outputs. To minimize the non-adiabatic loss, we propose a Symmetric Pass Gate Adiabatic Logic (SPGAL).To validate our proposed logic, we have evaluated the energy dissipation of the individual secure adiabatic logics; proposed CSSAL, secure adiabatic logic, symmetric adiabatic logic, 2N-2N2P. Furthermore, this work delves into the implementation of 2*2 multiplier operation using TFET at 0.3v. The bit parallel multiplier implemented using SPGAL saves up to 80% energy as compared to SQAL.**

Keywords-**Adiabatic, DPA, TFET, SPGAL.**

I. INTRODUCTION

DPA(Differential power analysis) is a type of attack that can reveal the secret key of a cryptographic device by analyzing the relation between the processed data and power traces [1]. The side channel attacks on cryptographic devices are considered as the most powerful because they can extract secret keys even when measured power traces are very noisy. There are many countermeasures against DPAs, such as architecture and algorithm level approaches [2], [3], but the circuit level approach is very attractive because it consumes constant currents for each computation, irrespective of employed security algorithms.

Adiabatic logic is one of the efficient circuit design techniques for designing energy-efficient hardware by efficiently recycling the charge stored in the load capacitor back to the power supply [4]. It is also used to design energy-efficient DPA-resistant hardware [5–10]. Among all the DPA-resistant adiabatic logic family of circuits proposed. the Secured Quasi Adiabatic Logic (SQAL) [9] is the most efficient in terms of power consumption and the area overhead. But, the drawback with SQAL is, it suffers from non-adiabatic energy loss during the evaluation of the outputs.

In this paper, a Symmetric Pass Gate Adiabatic logic is proposed. The proposed logic SPGAL reduces the non adiabatic loss during the evaluation of the outputs by making sure that there is no potential difference between the two nodes (source and drain) of the transistor when it is turned on. This paper investigates TFET based SPGAL which is ensured by balancing the supply peak current traces for all input transitions. The balancing of the peak current traces is performed by resetting the output values before the evaluation of the next cycle. To illustrate the design, SPGAL based adiabatic designs of buffer, XOR and NAND gates are illustrated in this work. The rest of the paper discusses the background and related work on DPA, adiabatic logic and DPA resistant adiabatic logic families. Further, the proposed SPGAL-based adiabatic logic gates are used to implement bit-parallel cellular multiplier over GF(2^2) using TFETS at 100MHZ.The proposed circuit design is simulated in cadence virtuoso environment and the results are analyzed and verified.

II. BACKGROUND

1. Tunnel Field Effect Transistor (TFET) - For low-power digital circuits TFETs are considered to be best choice. TFETs can able to achieve sub threshold swing below 60 mV/dec, enabling a high on-current to off-current ratio. Low Sub threshold Swing enables TFET to have low-leakage with higher performance than CMOS at lower voltage .In this work, we have used In As homo-junction tunneling FETs for our simulations. The main advantage of TFET is it can operate at very low supply voltages. In TFET, am -bipolar conduction is possible which reduces the ION current, and Increases the drain series resistance as well as process complexity. In this work, we have capitalized on the useful properties of TFET in designing DPA-resistant energy-recovery logic.

2. Energy Recovery Logic- Energy Recovery Logic employs power clock to effectively recycle the charge stored in the capacitor. This logic has very less dynamic switching energy loss because of the charge recycling mechanism. When a charge is supplied through constant current source the amount of energy dissipated in an energy recovery circuit is given by.

$$E=RC/T\ CVDD_{2} \qquad (1)$$

T denotes the charging /discharging of the capacitor, VDD is full swing of the power clock, C is the load Capacitor. The amount of energy dissipated by the Energy recovery logic is very less when compared to CMOS Circuits if T >> 2RC Which is time constant.

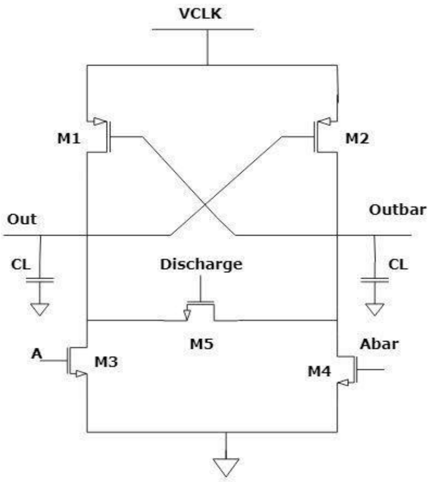

Fig.1 Sqal Buffer.

III.THE PROPOSED WORK

1. TFET based Secured Quasi Adiabatic Logic(SQAL)

A standard SQAL buffer is implemented using TFET and it is depicted in Figure3.1 a and the simulations are shown in Figure 3.1 b .They operates in four phases wait, evaluate ,hold and recovery. In wait phase input signals are generated and thus during evaluate phase input signals remain stable and outputs are calculated then the input signals goes low during hold phase while the power clock remains high and thus during the recovery phase the power clock goes low thereby, discharging the output nodes for energy recovery process.

Initially the out and out bar are at gnd. The main basis of this circuit is to devise the circuit for evaluate phase during the wait phase. There is a discharge transistor M5 which is added between internal nodes. During wait phase power clock is at gnd, discharge transistor is turned on which discharge the remaining charge stored so that there is no charge left over from the previously evaluated inputs and input A rises from 0 to 1 , With out non adiabatic loss the transistor M3 gets turned on. In evaluate phase power clock rises and the input remains stable .Here the transistor M1 and M2 gets turned on non adiabatically and the out gets charged. During this phase the buffer suffers from non adiabatic loss when the power clock reaches Vtp. In hold phase the output values will be hold. At recovery phase the charge stored in the output nodes gets recycled back to power clock. During the evaluation phase the circuit suffers from non adiabatic loss .SQAL XOR/XNOR gate consists of 9 transistors and the simulation results are shown in the Figure 3.1d .SQAL Nand gate is asymmetric in nature such that for each input signal the charge and discharge paths should be equal.

In NAND/AND gate there are three additional discharge transistors and in which the charge and discharge paths are data independent. However the number of transistor count in AND/NAND gate (15 transistors) is higher than that of XOR/XNOR (9transistors). The simulated waveform of SQAL AND/NAND gate is depicted in Fig.1 c. SQAL circuit does not leaks any information.

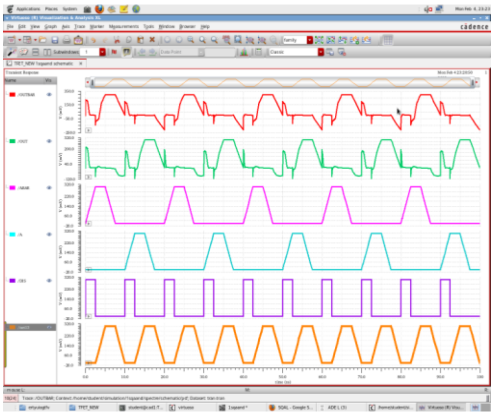

Fig. 2 SQAL Buffer Waveform.

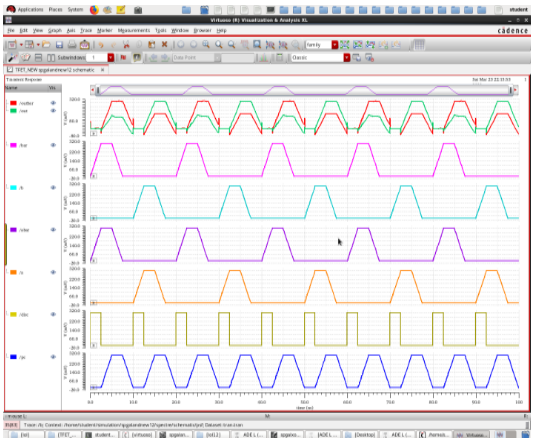

Fig. 3 SQAL AND/NAND Waveform.

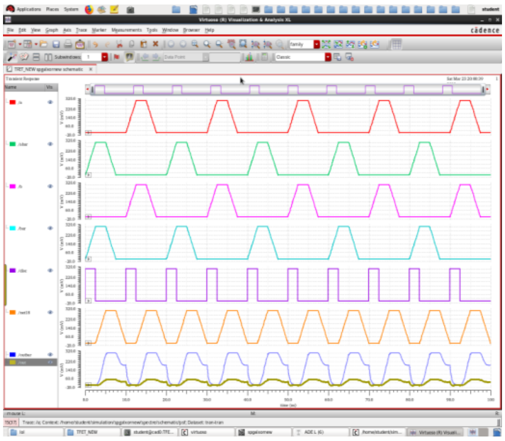

Fig.4 SQAL XOR/XNOR Waveform.

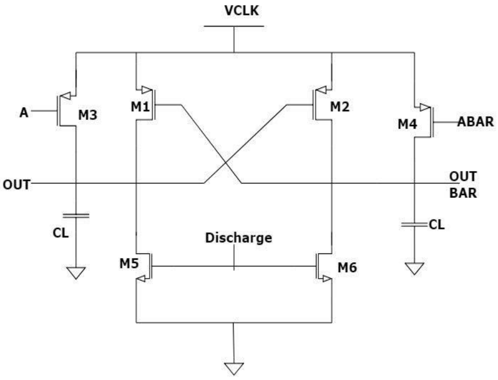

Fig.5 SPGAL Buffer.

2. TFET based Symmetric Pass Gate Adiabatic Logic: (SPGAL)

The proposed Symmetric Pass Gate Adiabatic Logic Buffer is implemented using TFET is a low power and DPA resistant energy recovery solution for Embedded Applications. TFET'S has low power consumption when compared to CMOS circuits due to the scaling of reduced supply voltage. The Schematic of the TUNSAL buffer is shown in Fig. 2 and the constant current traces are shown in fig. 3 The non adiabatic loss in SQAL buffer is eliminated in SPGAL buffer. With the help of buffer the operation is explained as follows.

Consider that all nodes are at gnd initially, when A=1 and Abar=0. During wait phase power clock is at gnd and the input signal A rises from 0 to Vdd and the transistor M3 gets turned on and the discharge signal gets turned on so that previous cycle output gets reset before the evaluation of the current cycle outputs. At Evaluate phase power clock rises high the current flows through M3 transistor to charge the load capacitor when the power clock rises from 0 to Vtp. The current flows through the transistors M3 and M1 to charge the load capacitor, when the power clock rises from Vtp to Vdd-Vtn.

When the power clocks arrives at Vdd-Vtn the transistor M3 is turned off and the current flows through the transistor M1 to charge the load capacitor. During hold phase input signal A decreases from Vdd to GND and out will be hold. At recovery phase power clock decreases from Vdd to GND. When power clock reaches from Vdd to Vtp. The charge gets recovered back through the transistor M1. As power clock arrives at Vtp, the transistor M1 is turned off and Cvtp charge gets stored in load capacitor. In wait phase Discharge signal is turned on in which the transistors M5 and M6 gets turned on to discharge the excess charge stored in the capacitor during the previous phase of the cycle. In every wait phase of the clock Discharge signal is turned on to discharge the redundant charge stored in the load capacitor.

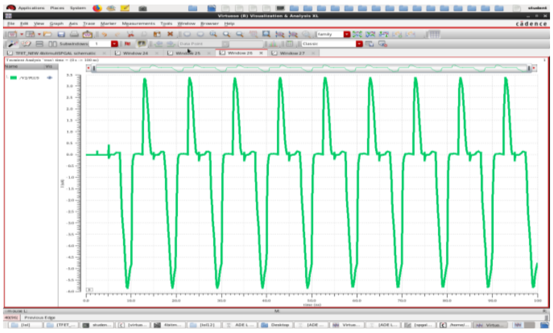

Fig. 6 SPGAL Buffer Constant Current Traces.

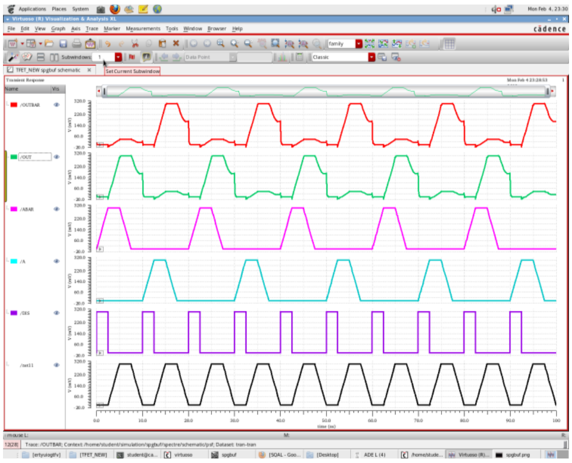

Fig. 7 SPGAL Buffer Waveform.

Due to the reduction of non adiabatic loss the TUNSAL is more energy efficient in nature when compared to other logic families. The simulation results of the proposed buffer is shown in figure 3.2c and the supply current traces waveform for different input transitions is shown in the figure 3.2 b proves that it is resistant to DPA attacks at the circuit level. The schematic of SPGAL based XOR/XNOR and AND/NAND gate is depicted in Figure 6 and 7.

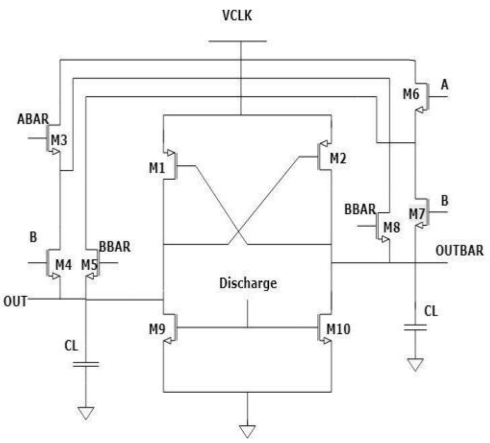

Fig.8 SPGAL XOR/XNOR.

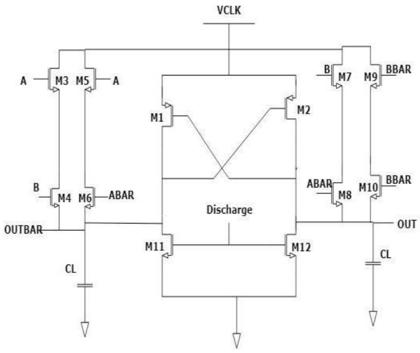

Fig.9 SPGAL AND/NAND.

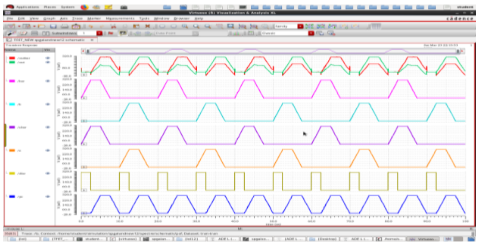

Fig. 10 SPGAL AND/NAND Waveform.

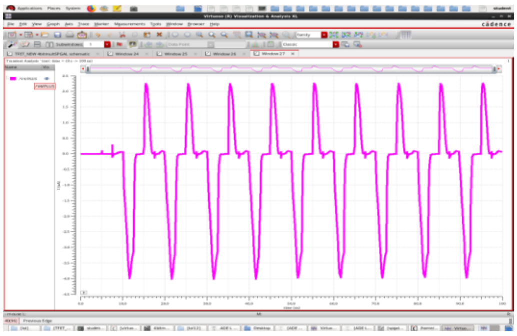

Fig.11 SPGAL AND/NAND Constant Current Traces.

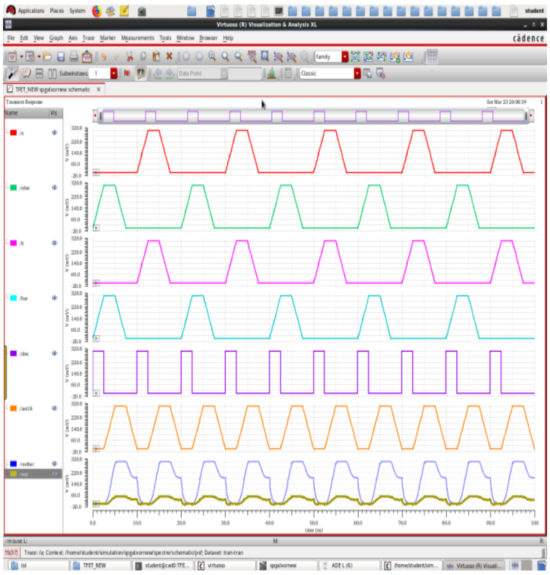

Fig.12 SPGAL XOR/XNOR Waveform.

3. TFET based Charge Sharing Symmetry Adiabatic Logic (CSSAL)

The charge-sharing symmetric adiabatic logic(CSSAL) inverter is proposed. The operation of CSSAL is shown in the following four phases:

1. Charge sharing - The discharge (Discharge) signal increases twice the rate of the input signal. In this phase, the power-clock voltage (Vpc) is stable at a low level, and the evaluation path signal which is established by In or In (MN5 or MN6) and Eval (MN8) cells, increases simultaneously and slowly. The total internal node capacitances are discharged to ground before the logic function is evaluated to prevent the circuit from depending on previous input data.

2. Evaluation phase - In the Eval phase, the Discharge signal is stable at a low level, which turns on MP1 so that the supply current can flow into the logic circuit. The output wires are evaluated through one ofthe active input cells.

3. Hold phase - During the hold phase, the current active input and Eval signals slowly decrease to a lower level; however, the outputs signals remain stable because these are controlled by the cross-coupled NMOSs MN1 and MN2.

4. Recovery phase - The power clock voltage (Vpc decreases to a low level, and the current active output discharges to a lower level via the active MP2 orMP3 and MP1 because the Discharge signal is still low. Consequently, charge recovery occurs for every power-clock cycle to minimize the energy lost during charging or discharging. The proposed CSSAL buffer transistor schematic is shown, in 3 and their simulation results shown in Figure 4.

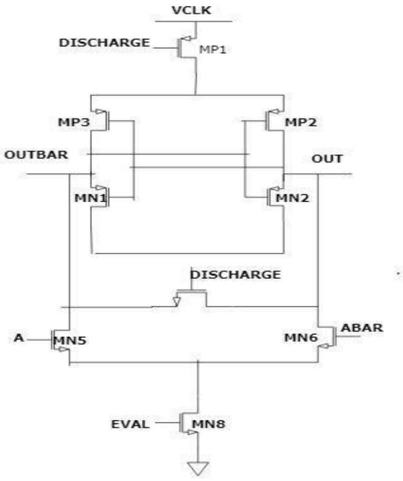

Fig. 13 CSSAL Buffer.

4. TFET based Symmetric Adiabatic Logic (SYAL)

The Syal Circuit uses power clock to recover the charge supplied and hence it saves power. When VCLK ramps down for energy recycling out or outbar gets discharged according to the VCLK.

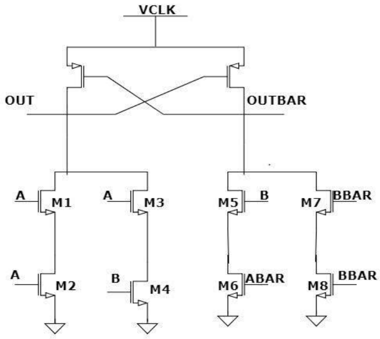

Fig.14 SYAL Buffer.

Here it gets discharged to voltage level not ground level depending upon the threshold voltage of the PMOS transistor. According to the charge stored in the nodes out and outbar, which depends on previous input data the supply current from VCLK varies.

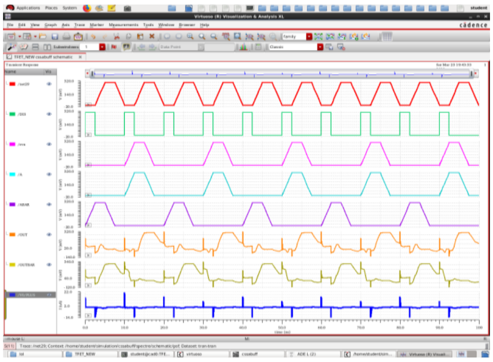

Fig.15 CSSAL Waveform.

5. TUNSAL based Multiplier

The proposed multiplier design explains the multiplier in the Composite field GF the 2 X 2 Multiplier in GF ((22)2) employs three SPGAL and and three SPGAL Exor gates. The principle involved in this design is Galois Field Arithmetic. In Cryptography Galois Field plays a very crucial role. It plays a very important part in modern cryptography Algorithms. It is represented with the notation GF(pn) ,where p denotes prime prime number and n is a positive number. For the construction of hardware circuit design p=2 is very suitable for finite field Multipliers.GF(2).

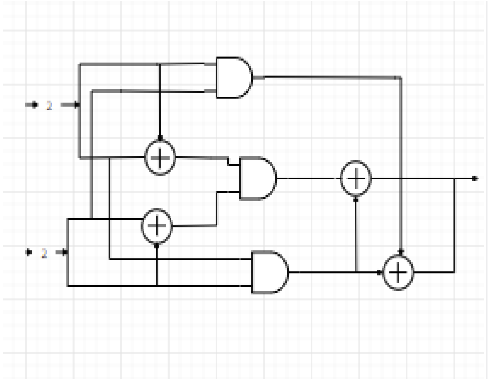

Fig.16 2x2 Bit Parallel Multiplier.

Can be denoted using signals 0 and 1. The finite field consists of one primitive element, zero element, unit element and has one primitive irreducible polynomial which is represented by the equation, $p(x)=x_n + p_{n-1}.x_{m-1}..+..+p_1+p_0$ hence GF(2) associated with it. The simulated results are performed using cadence virtuoso environment at 0.3 v and the uniform supply current traces of the multiplier shown in Figure 3.5 a proves that the bit parallel multiplier implemented using SPGAL logic family is secure against side channel attacks. The simulated results of the bit parallel multiplier are depicted in Fig.15.

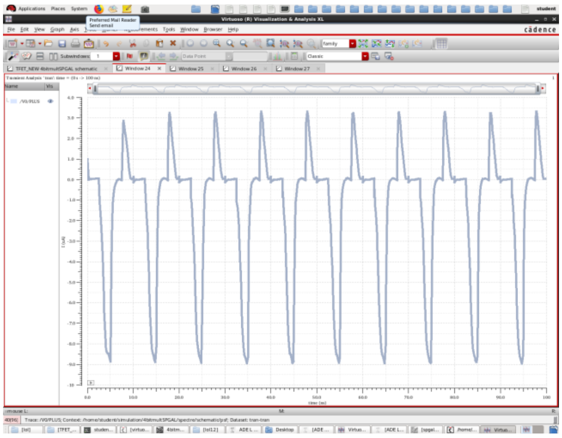

Fig.17 Constant Current Traces of bit parallel multiplier.

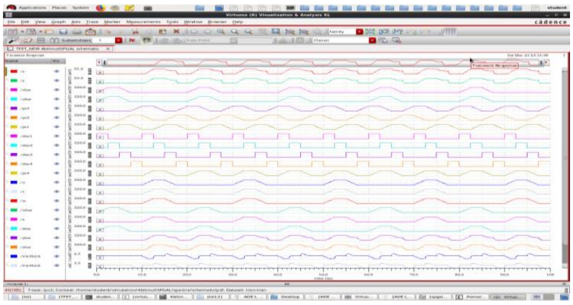

Fig.18 Bit parallel Multiplier Waveform.

IV.RESULTS

Based on the implementation of different secured adiabatic logic proposed using TFET the power has been calculated for individual Circuits and the average Energy consumed is calculated and the result are shown in Table 1.

Table 1 Power Analysis for Different Logic Families.

Logic Family	Logic Gate	Average Energy (100 MHZ)(FJ)
SPGAL	Xor/Xnor And	5.85 9.40
SQAL	Xor/Xnor And	26.44 44.08
CSSAL	Xor/Xnor And	16.87 16.48
SYAL	Xor/Xnor And	8.58 14.42

From the calculations of Average Energy consumed for different secured adiabatic circuits it is proven that SPGAL has better Energy savings when compared to other logic circuits and based on the constant current traces we obtained for SPGAL Circuits for different input transitions it is been proven that SPGAL is more secure when compared to SQAL. As the SQAL suffers from non adiabatic loss and this loss is eliminated in SPGAL. The width of Pmos and Nmos transistors are 0.9:0.18.

V. CONCLUSION

Energy recovery computing in TFET is a promising platform for low power and it provides increased DPA resistance with minimal power consumption. TUNSAL gates offer superior security with low power consumption as compared to CMOS gates .The width used for pmos and nmos transistors are 0.9:0.18. It is been proven that SPGAL logic is more energy efficient and it consumes less power when compared to other logic families. Due to the low power consumption and resistant against DPA attacks makesTFET based SPGAL promising candidate to implement in DPA resistant devices. Furthermore this work delves into the implementation of 2*2 multiplier using SPGAL gates using TFET and the constant current traces are obtained for the SPGAL based Multiplier proves that the system is resistant to DPA attacks. The proposed work is suitable for applications like RFID Tags, Smart Cards, and Embedded Applications.

REFERENCES

[1]. W. Cheng, S. Wang, X. Cheng, Virtual track: applications and challenges of the rfid system on roads, IEEE Netw. 28 (January (1)) (2014) 42–47.

[2]. E. Shi, A. Perrig, Designing secure sensor networks, IEEE Wirel. Commun. 11 (December (6)) (2004) 38–43.

[3]. A. Moradi, A. Poschmann, Lightweight cryptography and dpa countermeasures: a survey, in: Financial Cryptography and Data Security, Springer, Tenerife, Canary Islands, Spain, 2010, pp. 68–79.

[4]. P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in Cryptology – CRYPTO'99, Springer, Santa Barbara, California, USA, 1999, pp. 388–397.

[5]. W.C. Athas, L.J. Svensson, J.G. Koller, N. Tzartzanis, E.Y.-C. Chou, Low-power digital systems based on adiabatic-switching principles, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2 (4) (1994) 398–407.

[6]. M. Khatir, A. Moradi, Secure adiabatic logic: a low-energy dpa-resistant logic style, IACR Cryptol. ePrint Arch. 2008 (2008) 123.

[7]. B.-D. Choi, K.E. Kim, K.-S. Chung, D.K. Kim, Symmetric adiabatic logic circuits against differential power analysis, ETRI J. 32 (1) (2010) 166–168.

[8]. C. Monteiro, Y. Takahashi, T. Sekine, Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks, in: 2013 36th International Conference on Telecommunications and Signal Processing (TSP), IEEE, Rome, Italy, 2013, pp. 732–736.

[9]. M. Avital, H. Dagan, I. Levi, O. Keren, A. Fish, Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes, IEEE Trans. Circuits Syst. I: Regul. Pap. 62 (1) (2015) 149–156.

[10]. H. Thapliyal, M. Zwolinski, Reversible logic to cryptographic hardware: a new paradigm, in: 2006 49th IEEE International Midwest Symposium on Circuits and Systems, vol. 1, IEEE, San Juan, Puerto Rico, 2006, pp. 342–346.

[11]. S.D. Kumar, 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, Oak Ridge, 2016.

[12]. S. Mangard, E. Oswald, T. Popp, Power analysis attacks: revealing the secrets of smart cards, Springer Science & Business Media, vol. 31, 2008.

[13]. S.D.Kumar,H.Thapliyal,A.Mohammad,andK.S.Perumalla,“Design exploration of a symmetric pass gate

adiabatic logic for energy-efficient and secure hardware,” Integration, the VLSI Journal, 201