Energy Efficient Adiabatic Logic Circuit for Improve Security in DPA Resistant RFID

A G Vaishiba¹, Dr. Ananiah Durai²
School of Electronics Engineering, VIT, Chennai¹,²
ananiahdurai.s@vit.ac.in²

Abstract
A Differential Power Analysis (DPA) attack is an exploit which overcomes the hardware and software security by analyzing the correlation between electricity usage of a chip in a device and the encryption key. These attacks are non-invasive, leading an intruder to crack a system without leaving any trace. CMOS Technology is prone to DPA attack because of higher power dissipation. A DPA resistant adiabatic technique has been analyzed which has lower power dissipation when compared to the CMOS technology. The conventional Positive Feedback Adiabatic Logic (PFAL) suffers from certain non-adiabatic energy loss. Hence, Energy Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is proposed which reduces the non-uniform power consumption, preventing information leakage thus securing the system from DPA attacks. Thus the proposed EE-SPFAL is used to design logical circuits such as buffer, OR-XNOR and AND-NAND gate. It is proved that the information leakage in the form of current consumption takes place in PFAL buffer whereas current consumption traces in EE-SPFAL circuits are uniform, depicting the ability of the proposed logic family to resist DPA attack. The simulation was done using Cadence virtuoso 180 nm technologies.

Keywords: DPA Attack, Adiabatic Logic, Energy Efficient and Secure, Current Trace, Information leakage

1. Introduction
An important role is played by the adiabatic technique in portable devices present with constrained battery life. Long lasting battery requirement of devices can be approached by analyzing adiabatic logic. Enhancing the battery life of devices styles are devised out of which the most promising technique adiabatic logic till date. As the demand of hand held devices increases, it demands in need for promising power battery life. Moreover ICs of this generation work at enormous high speed revealing more switching activities due to which they happen to dissipate large power and causing heating up of device, forcing manufacturers to use bulky heat sinks. Thus ways to optimize the area overhead along with power consumed is to be implemented. Heating up due to power dissipation is a main problem when it comes to portability. Power dissipations in CMOS circuits are:

- **Dynamic Power Dissipation**: the power consumed by any device during its switching operation. Power which is dynamic consists of short-circuit power.
- **Static Power Dissipation**: the power consumed when the system is in standby mode or when
is not powered. Various strategies are available at different levels in VLSI design process for optimizing the power consumed. The speed is consequently reduced using supply voltage scaling. Thus, the adiabatic logic technique is explored in this paper to reduce the dynamic power.

1.1 Adiabatic logic

In thermodynamic system, this term means no heat transfer from environment to the system and vice versa. Adiabatic logic is popularly known as ‘energy recovery logic’ as it reuses the energy. It shows that the dissipating stored energy during the charging process can be recycled, the energy is sent back to the power supply thus the power dissipation is reduced. This term ‘Adiabatic Logic’ is used to express the switching circuits that can be operated without losses, and the term ‘Semi Adiabatic circuits’ is used to show the switching circuits that operates with a power lesser than that of conventional CMOS circuits, such adiabatic switching based circuits still might have some non-adiabatic losses. In both scenarios, the term is used to show that these circuits are capable of operating with substantially loser power dissipation than conventional CMOS switching circuits.

The adiabatic logic follows the bellow rules:
- Turning switches off when no current is flowing through them
- Turning switches on when there is no potential difference between them
- Using a power supply that is capable of recovering or recycling energy in the form of electric charge.

2. Positive feedback adiabatic logic (pfal) buffer

2.1 Circuit Design

The logic buffer was designed using PFAL logic as shown in Figure 1. This methodology is not very secure towards DPA attack as there is high correlation between the processed data and the current traces from the supply source of the circuit. Hence results in information leakage.

![Figure 1. Schematic of PFAL Buffer](image-url)
When there is non-uniform current consumption, it signifies information leakage. This current consumption in a non-uniform pattern is due to redundant charges present, which must be avoided. Information leakage in the form of supply current traces of the PFAL buffer is shown in Figure 2.

2.2 Simulation results
The simulation result of PFAL buffer is shown in Figure 3 where on passing the input at “a” the same was obtained at the output, thus verifying the functionality of the buffer. The drawback in this adiabatic logic is that all the charges stored in the load capacitor will not be recovered and these redundant charges will result in non-uniform current consumption which implies information leakage. Thus this design acts as low power hardware while compromising in security.
3. Energy efficient secure positive feedback adiabatic logic (eesspfa) buffer

3.1 Circuit Design

To overcome the drawback of PFAL logic and make it more energy efficient as well as secure EESPFAL was proposed. This ensures that the correlation between data processed and the current traces of the supply be reduced. DPA attack was possible by analyzing the pattern in power consumption, thus by restricting such analysis makes this design secure. The reductant charges present in the capacitors which were not completely removed pave way to non-invasive extraction of cryptographic keys from any device. This was done by the means of discharging or removing the redundant charges stored in the load capacitor by means of a “discharge” signal. The schematic of EESPFAL buffer with additional signal “discharge” is shown in Figure 4.

![Figure 4. Schematic of EESPFAL Buffer](image.jpg)

The current traces for the input supply in EESPFAL will be uniform as the redundant charge from the 50pF load capacitance is discharged using “discharge” signal. The supply current traces is shown in Figure 5.

![Figure 5. Current traces of EESPFAL Buffer’s source voltage](image.jpg)
3.2 Simulation results
The simulation result of EESPFAL buffer is shown in Figure. 6, where, the output is obtained as such at the input thus verifying the buffer’s functionality. The side channel DPA caused by power analysis is eradicated using this adiabatic logic. The discharging of redundant charges happens in a smooth manner making this design secure by preventing information leakage. Thus the analyzed design is not only energy efficient but also secure from DPA attack caused by correlation of data processed with current traces of the device.

![Figure 6. Transient Waveform of EESPFAL Buffer](image)

4. Comparison of energy consumption by pfal and eespfal buffer
The energy consumption is both the buffer designs were calculated and it was noticed that the EESPFAL buffer is more energy efficient than PFAL buffer as shown in Table.1.

| Adiabatic Logic   | Energy Consumed (J) |
|-------------------|---------------------|
| PFAL Buffer       | 3.524 × 10^{-15}    |
| EESPFAL Buffer    | 9.908 × 10^{-15}    |

5. Eespfal and/nand, xor/xnor logic gate implementation
5.1 Circuit Design
Using the EESPFAL method an energy efficient and secure AND/NAND and XOR/XNOR logic gate was designed which had four inputs (a, b, abar, bbar) and two outputs (and, nand & xor, xnor) respectively. The circuit as shown in Figure .7 implemented AND logic on the left hand side and NAND logic on the right hand side respectively whereas the circuit as shown in Figure. 8 implemented XOR logic of the left side and XNOR on the right side. Load capacitors of 50fF were used on both the sides of the circuit. Both the circuits also had the “Discharge” signal to remove the redundant charges stored in the load capacitors to cause uniform current consumption and prevent information leakage.
5.2 Simulation results
After providing a certain combination of inputs the AND/NAND & XOR/XNOR logics were verified by performing the transient analysis, the waveforms as shown in Figure 9 were obtained for AND/NAND logic circuit. The functionality of the XOR/XNOR logic circuit was also checked as shown in Figure 10 and it was found to be energy efficient.
5.3 Normalized Energy Deviation (NED) Analysis for AND and XOR Gate

By obtaining the values of maximum and minimum energy utilized by the inputs of AND and XOR gate to find out the energy deviation in the circuit by using the formula

\[(E_{\text{max}} - E_{\text{min}})\]  

(1)

This depicts the percentage change in maximum and minimum energy for various input transitions. From Table 2 it can be seen that the NED for both EESPFAL XOR and AND gates are less than 1 percent. This indicates the ability of these logic families to resist the DPA attack and be secure.

Table 2. Energy consumed by AND and XOR gate

| Energy Consumed | EESPFAL AND | EESPFAL XOR |
|-----------------|-------------|-------------|
| Emin (pJ)       | 0.25        | 0.19        |
| Emin(pJ)        | 0.29        | 0.21        |
| NED(%)          | 0.137       | 0.095       |
6. Adiabatic logic based full adder circuit

6.1 Circuit Design
A full adder is a combinational circuit performing arithmetic sum of three inputs (a, b and cin). Here the schematic is divided into two- sum circuit and carry circuit to obtain the respective outputs. The schematic of sum circuit is as shown in Figure 11 and the schematic for carry are as given in Figure 12.

![Figure 11. Schematic of sum circuit of full adder](image1)

![Figure 12 Schematic of carry circuit of full adder](image2)

6.2 Simulation results
The sum and carry functionalities are verified by means of analyzing the transient analysis of their respective circuits. The waveform of sum circuit is as shown in Figure 13. The transient analysis of circuit carry is depicted in Figure 14.
Figure 13. Transient waveform of sum circuit

Figure 14. Transient waveform of carry circuit

7. Conclusion

The various adiabatic logic circuits were analyzed using CMOS 180nm cadence technology. The EESPFAL enabled proper switching of transistors and resulted in reduction of non-adiabatic energy loss. It disrupted the correlation between data processed by the circuit and the current traces from the power consumed by the respective circuit, making it DPA resistant.

8. References

[1] M Avital, H Dagan, I Levi, O Keren and A Fish 2015 DPA-secured quasi adiabatic logic (SQAL) for low-power passive RFID tags employing sboxes *IEEE Trans. Circuits Syst.* 149–156.

[2] C C Sun, C C Wang and M H Sheu 2014 Ultra Low Power Circuit Design Based on Adiabatic Logic 2014, Tenth *International Conference on Intelligent Information Hiding and Multimedia Signal Processing* pp. 317-20.
[3] C Monteiro, Y Takahashi, and T Skein 2013 Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level *Microelectronics. J* pp. 496–503.

[4] K Kumar, D Somasundareswari, D Duraisamy and G Sabarinathan 2013 Asynchronous design of energy efficient full adder *International Conference on Computer Communication and Informatics* pp. 1-6.

[5] A K Maurya and G Kumar 2011 Energy Efficient Adiabatic Logic for Low Power VLSI Applications *International Conference on Communication Systems and Network Technologies*, pp. 460-63.

[6] B D Choi, K E Kim, K S Chung and D K Kim 2010 Symmetric adiabatic logic circuits against differential power analysis *ETRI J* pp. 166–168.

[7] M Moradi, T M Shalmani, and M Salmasizadeh 2009 Dual-rail transition logic: A logic style for counteracting power analysis attacks *Comput. Electr. Eng.*, pp. 359–69.

[8] M Khatir and A Moradi 2008 Secure adiabatic logic: A low-energy DPA resistant logic style *IACR Cryptology* Art. No. 123.