International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Low Power Security System by Using Dral

B. Rashika[1], R. Ramadoss[2]

[1]P.G Scholar, Department of Electronics and Communication Engineering, Sri Muthu Kumaran Institute of Technology Chennai, Tamilnadu, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Sri Muthu Kumaran Institute of Technology Chennai, Tamilnadu, India

Abstract : ***Power dissipation in modern technologies is an important issue, and overheating is a serious concern for both manufacturer and customer. Everyday new technology which is faster, smaller and more complex is being developed .. This paper describes a side channel attack resistant coprocessor IC fabricated .The IC is being developed with both Reversible and Adiabatic logic and is been proposed with 180nm CMOS technology.. Reversible logic is used due to its less heat dissipating characteristics. Adiabatic logic (DRAL) 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 .It is capable of both forward encryption and reverse decryption by using AES algorithm for security applications. The Adiabatic logic with reversible technique is used and simulated in HSPICE. This technique is also used in allowing for efficient hardware reuse.***

Keywords: Adiabatic logic, Reversible gates, AES algorithm, DPA DRAL

1. Introduction

This work focuses on the reduction of the power dissipation, delay, size and securities. The implementation of Adiabatic Dynamic Differential Logic for applications in secure IC design for stronger mitigation of DPA attacks[11]. These systems dissipate energy due to bit erasure within their interconnected primitive structures, which is an important consideration as transistor density increases. The Advanced Encryption Standard (AES) provides a symmetric key cryptography that allows for the encryption and decryption of fixed size blocks of data. As a symmetric system, the secret key must be shared between the sender and receiver in order for communication to be possible. In order to design an ideal universal computer that dissipates arbitrarily-low energy, reversible logic must be implemented. Adiabatic circuits are low power circuits which use "reversible logic" to conserve energy. Unlike traditional CMOS circuits,[13] which dissipate energy during switching, adiabatic circuits attempt to conserve charge . Adiabatic logic works with the concept of switching activities which reduces the power by giving stored energy back to the supply. Thus, the term adiabatic logic is used in low-power VLSI circuits which implements reversible logic.[1] In this, the main design changes are focused in power clock which plays the vital role in the principle of operation. Reversible computing is generally considered an unconventional form of computing. There are two major, closely related, types of reversibility that are of particular interest for this purpose: physical reversibility and logical reversibility. This method improved upon SCRL and ECRL by significantly reducing the overhead required to perform evaluation and discharge, as well as improving the signal propagation. More generally, reversible gates have the same number of inputs and outputs.

2. AES Encryption Algorithm

With the advent of easily available high speed computers there has been an increase in demand for effective methods to secure data. Older cryptographic methods, such as DES, do not have a large enough key space to lend themselves to applications where high security is needed. Advanced Encryption Standard (AES) provides a symmetric key cryptography that allows for the encryption and decryption of fixed size blocks of data[3]. The major steps involved in each round of encryption are the Byte Sub, Shift Row, Mix Columns, and Add Round Key .

2.1 Sub Byte

The Byte Sub operation performs a byte substitution on every byte of data in the current state[12]. A representation of the Byte Sub operation

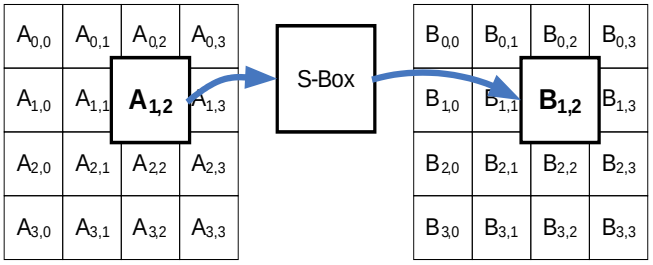

Figure 2.2: S-box Operates on Individual Bytes

2.2 Shift Row

The Shift Row operation affects each of the four rows of data individually. Each row is rotated by a different amount. The first row is unchanged and rows two through four are rotated by one, two, and three bytes respectively. For encryption a right rotation is performed while for decryption a left rotation is used[10]. The result of the shift on the data matrix representing the data

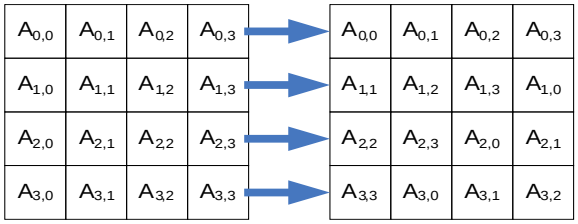

Figure 2.3: Left Rotation Used for Decryption

2.3 Mix Column

The Mix Columns operation transforms the data in the current state by operating on each of the four columns independently.

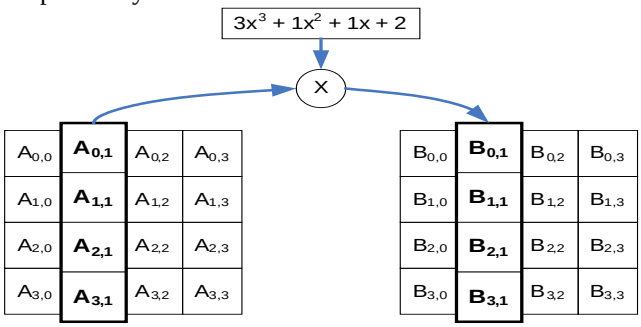

Figure 2.4: Mix Column Operation

2.5 Add Round Key

The Add Round Key operation performs a simple XOR between the current state data values and the round key for the current round [11]. The round key is obtained from the key selector block based on the value of the expanded key

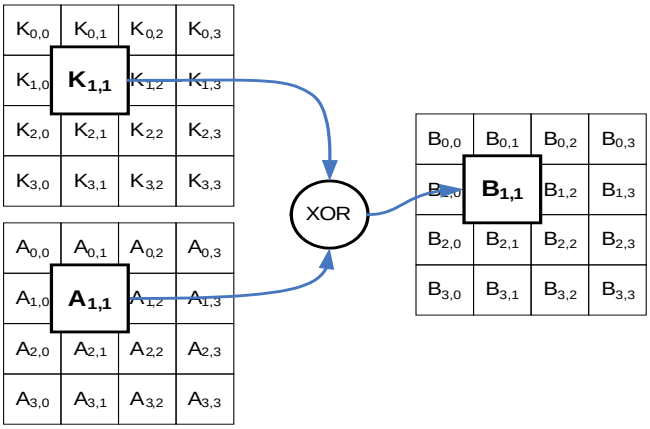

Figure 2.5: Round Key Bytes (K) XOR with Data Bytes (A)

2.6 Reversible Circuit

A reversible logic gate is an n-input n-output logic device with one-to-one mapping. This helps to determine the outputs from the inputs and also the inputs can be uniquely recovered from the outputs. Also in the synthesis of reversible circuits direct fan-Out is not allowed as one–to-many concept is not reversible[1]. However fan-out in reversible circuits is achieved using additional gates. A reversible circuit should be designed using minimum number of reversible logic gates. From the point of view of reversible circuit design, there are many parameters for determining the complexity and performance of circuits The number of Reversible gates (N): The number of reversible gates used in circuit [4].The number of constant inputs (CI): This refers to the number of inputs that are to be maintained constant at either 0 or 1 in order to synthesize the given logical function. The number of garbage outputs (GO): This refers to the number of unused outputs present in a reversible logic.

2.7 Adiabatic Logic

The main obstacle to using adiabatic logic in computing design is that complete adiabaticit means absolutely zero rate of entropy generation[5]. There are two issues that must be addressed in any adiabatic circuit. First, the implementation must result in an energy-efficient design of the combined power supply and clock generator. Second, reversible logic functions require greater logical value[6]. Therefore, the energy dissipated by switching of the circuit must be controlled and recycled instead of dissipated into the environment. . This issue was addressed using Split-Level Charge Recovery Logic (SCRL),Efficient Charge Recovery Logic (ECRL) .Truly adiabatic circuits require that the output signals may be placed on the outputs and the unique input signals may be reproduced on the input wires. A dual rail approach was used to accomplished this goal . In this, the main design changes are focused in power clock which plays the vital role in the principle of operation. Each phase of the power clock gives user to achieve the two major design rules for the adiabatic circuit design.

• Never turn on a transistor if there is a voltage across it (VDS>0)
• Never turn off a transistor if there is a current through it (IDS≠ 0)
• Never pass current through a diode

2.7.1 DRAL

EEAL requires only one sinusoidal power clock supply has simple implementation and performs better than previously proposed adiabatic logic families in terms of energy consumption. Ass single-clock circuit requires simple clock scheme [2], this logic style can enjoy minimal control overheads.

3. Simulation Results

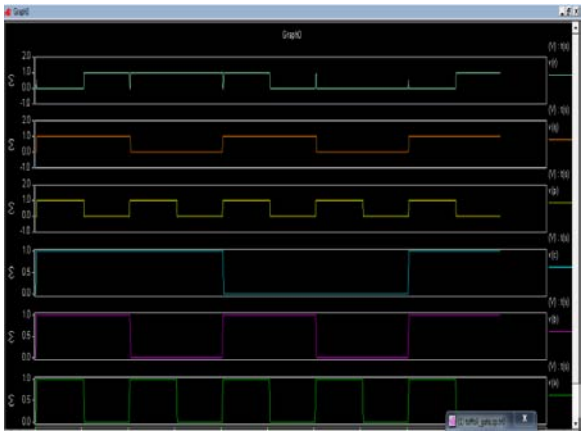

Figure 3.1: Snapshots for proposed Toffoli gate

The difference in power is accounted for in the degraded output signal of the non-body biased Toffoli gate. Since

there is no body biasing, the output signal for toffoli gate is given with transient analysis . The more the signal is degraded, the more the reversibility of the circuit is compromised. As a result, the energy dissipation and power consumption of the device increases. Signal ABC are considered as the input and PQR has the output.The result is verified using the Truth table of TOFFOLI gate

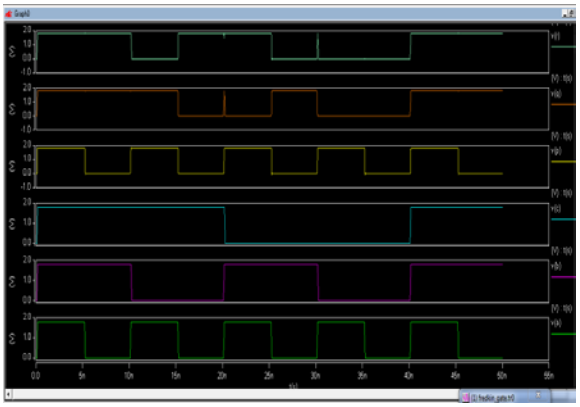

Figure 3.2: snapshot for fredklin gate

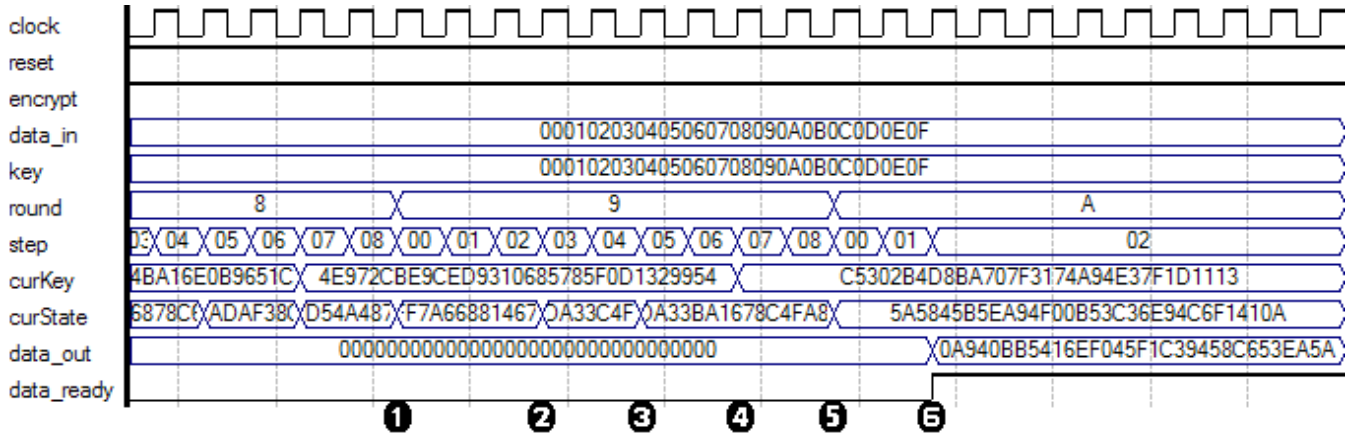

Figure 3.3: snapshot for AES

In the shown waveform there are several things that can be seen. The beginning of a the final round can be seen at point 1 . Following this, the update from the current state to the result of the ByteSub operation can be seen at point 2 . The next update to the result of the ShiftRow operation is shown at point 3. Since this is the final round, the Mix Column operation is skipped. However, at the same point 4 where the Mix Column operation is performed during other rounds the current key is still updated, and this can be seen at point 5. The final result of the last rounds computation can be seen at point 6. The final mark at point shows the results of applying the data mapping to achieve the proper format before placing the results on the output port.

Comparison Table

S.No	*Parameters*	*Existing*	*proposed*
1	Power	47.186µw	23.6290µw
2	Delay	5.19ns	2.570ns
3	Power delay product	51.8115f	31.3410f
4	Peak power	454.489µw	216.48µw

4. Conclusion and Future Work

Here address two major debates in reversible logic. First, we present an adiabatic source-memory device in CMOS which operates at operation of the ‘‘0’’ and ‘‘1’’. This circuit is presented as a case study that switching circuits are not required to consider charge as a state, since the copy operation of the memory device allows for energy recycling. Measurement of the CMOS value does not necessarily result in energy dissipation. Therefore, adiabatic switching is used in charge based computing by properly modifying local reversible CMOS based structure. we use DRAL to improve the operation of adiabatic CMOS logic structures. Simulations in HSPICE using 180nm predictive technology is showed This DRALmethod was applied to adiabatic Toffoli gate and fredklin gate. The most significant tradeoff is operating frequency. The reversible property of the dual-rail adiabatic circuit to allow for design reuse for both encryption and decryption, which is not physically possible in all the previous concepts.

References

[1] R. Wille, D. GroSSe, G. Dueck, and R. Drechsler, “Reversible logic synthesis with output permutation,” in Proc. 22nd Int. Conf. VLSI Design, New Delhi, India, Jan. 2009,

[2] Kioi, K.; Kotaki, H.; Kakimoto, S.; Fukushima, T.; Sato, Y., "Forward body-bias CMOS dual rail logic using an adiabatic charging technique with sub -0.6 V operation," Electronics Letters , vol.33, no.14, pp.1200,1201, 3 Jul 1997.

[3] P. Hämäläinen, T. Alho, M. Hännikäinen, and T. D. Hämäläinen, “Design and implementation of low-area and low-power AES encryption hardware core,” in Proc. 9th EUROMICRO Conf. DSD, Dubrovnik, Croatia, Aug. 2006

[4] G. P. Boechler, J. M. Whitney, C. S. Lent, A. O. Orlov,and G.L.Snider, “Response to comment on‘Fundamental limits of energy dissipation in charge-based

[5] Anuar, N.; Takahashi, Y.; Sekine, T., "Fundamental logics based on two phase clocked adiabatic static CMOS logic," Electronics, Circuits, and Systems, 2009. ICECS 2009.
[6] I. E. Sutherland and R. F. Sproull, “Logical effort: Designing for speed on the back of an envelope,” in Proc. Univ. California/Santa Cruz Conf.Adv. Res. VLSI 1991, pp. 1–16.
[7] H. El-Masry and D. Al-Khalili, “Cell stack length using an enhanced logical effort model for a library-free paradigm,” in Proc. 18th IEEE Int. Conf. Electron. Circuits Syst., Dec. 2011,
[8] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolic, Digital Integrated Circuits: A Design Perspective. Upper Saddle River, NJ, USA: Prentice- Hall, 2003, p. 761.
[9] A. Razafindraibe and al. “Secured structures for secured asynchronous QDI circuits” in XIX Conference on Design of Circuits and Integrated Systems (DCIS’04), Nov. 24-26, 2004
[10] K. Tiri and al. “Securing encryption algorithms against DPA at the logic level: next generation smart card technology”,Cryptographic Hardware and Embedded Systems Workshop, September 8-10, 2003
[11] K. Tiri and al. "A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs," date, pp. 58-63, Design, Automation and Test in Europe (DATE'05) Volume 3, 2005.
[12] F. Mace and al. “A dynamic current mode logic to counteract power analysis attacks”, DCIS 2004.
[13] P. Maurine and al, "Transition time modeling in deep submicron CMOS" IEEE Trans. on CAD, vol.21, n11, pp.1352-1363, 2002.