Analytical Modelling of Hybrid CMOS SET Rijndael Cryptography

J. Gope, S. Chowdhury, S. Chakraborty and S. Bhadra

Abstract Hybrid CMOS-SET has come up as a promising candidate for next generation ultra small, digitized, low power consuming and high speed Nano device to replace the conventional CMOS electronics. Researchers since last decade exhibitedtheir skill to develop Hybrid CMOS-SET based Nano ICs. Also contemporary research aims to incorporate the same Nano ICs in consumer electronics, health diagnostic systems as well as in cyber security. Few attempts have been made so far to fabricate nm ICs for ultra modern cyber security systems. CMOS made Rijndael cryptographic hardware is ubiquitous today, because of its excellent encryption standard. In order to model the hardware in nm region the authors here report an empirical study to implement hybrid CMOS-SET based Rijndael IC. The proposed architecture is a nm ASIC which resembles high speed during encryption beside other novelties.

1 Introduction

Post CMOS era envisaged the resurgence of numerous nano scale devices. Amid which quantum electronics plays a pivotal role in optimizing new principle of operation of molecular scale electronics. But owing to its typical material and process related limitations quantum electronics suffered serious setback. The technological shift then tends towards a new device principle where freedom of electronics was of utmost credibility. This is known as Single Electron Technology (SET) [1]. Single electronics is a fascinating technology which involves greater figure of merit deliberated from high integrating density, low power consume-ability, high processing speed, simplicity, straight forwardness, robustness and of course the potentiality to uphold one bit of information using few electrons

J. Gope (✉) · S. Chowdhury · S. Chakraborty
Department of ECE, CSET, Barasat, Kolkata, West Bengal 7000124, India
e-mail: jayanta.gope.1983@ieee.org

S. Bhadra
Department of EE, UEM, Saltlake, Kolkata, West Bengal 700156, India

I. Bhattacharya et al. (eds.), *Advances in Optical Science and Engineering*,
Springer Proceedings in Physics 194, DOI 10.1007/978-981-10-3908-9_59

or a single electron. Besides, the fragility of single electronics is that the fabrication can not be obtained at room temperature operation maneuver and also it posses random background charge problem, low gain, high output impedance. This feared the Scientist that might SET alone could not replace CMOS in future VLSI/ULSI circuit design.

On the other hand CMOS is well studied since the 70s and thus a vibrant technological enhancement is omnipresent. This methodically aids a device engineer in prolific CMOS based logical designing. CMOS intrinsically foster high gain; can be operated within room temperature, does not propagate any background charge and also the speed power product lies in proximity to the Heisenberg's principle. The cosmic effects are quite relevant. Combining the goodliness of CMOS and SET, Scientist introduced a co-integrated model that diminishes the flaw of both CMOS and SET and thus Hybrid CMOS SET [2] was conceptualized. Presently Hybrid CMOS SET made novel architecture mimic the Boolean logic and categorically several Hybrid CMOS SET made logic realizations are reported [3].

On the other hand the role of internet is ubiquitous in today's era. This has augmented the electronic financial transfer system manifold. Subsequently to maintain the internet security cryptography is utmost essential. It is the technique of sending and receiving data in a concealed form so that only the specific receiver can read and process it. It facilitates inbound security to the every concerned even. It also maintains data integrity, confidentiality and authentication. In this regard all over the world, different algorithms were made available in cryptography. In 1997, the National Institute of Standards and Technology (NIST) initiated a programme to select a suitable algorithm on cryptography and in 1998, NIST announced the acceptance of 15 algorithms and after that they selected 5 as finalist. Among them Rijndael Algorithm which was designed by Joan Deemen and Vincent Rijmen, was unanimously accepted as Advanced Encryption Standard (AES) [4] in 2000. AES selects this model depending upon a number of properties such as performance, efficiency, security, flexibility and easy to implement. Additionally, this model was simulated using VHDL since its very inception. Overall this algorithm offers excellent key set up time and well key agility and also requires less memory. Owing to its unmatched advantages, authors opted to design Hybrid CMOS SET based Rijndael model.

Basically, the author here tends to incorporate Hybrid CMOS SET in a new paradigm of cyber security based cryptographic hardware realization and henceforth submit this ephemeral architecture of Hybrid CMOS SET Rijndael circuit.

2 Modelling of Rijndael Algorithm

Rijndael algorithm is unputdownable in cryptography due to some of its features like simple design technique, good speed, withstand against hacking and code compactness. For exquisite performance the algorithm uses different input block lengths like 128, 192 and 256 bits. Additionally the algorithm employs different

key length and different number of rounds depending upon its block length as enunciated in the Table 1.

The entire encryption process is done subsequently in four steps [5, 6]. It initiates with 'Add Around Keys'. In this operation simple XOR function is applied between the 'State' and the 'Round Key'. The Round Key is derived from the 'Cipher Key' by Key Scheduling Technique. Besides 'State' is a simplistic but straight forward array of bytes having four rows and the number of column is equal to the block length divided by 32 intervals. The state and Round Key have the same size for this purpose. Consequently a new state is obtained following the operation

$$S(i,j) = S(i,j)\,K(i,j) \tag{1}$$

where S is the state and K is the Round Key.

This is followed by Sub Byte Transformation. Thus it is a non linear bit wise substitution of each state bit in independent arbitration. Rijndael algorithm offers only one Substitution Table defined as S-box. The designing process of S-box is such that it can prevail over attack.

Last but not least is Shift Row Transformation. Here the rows of the state are cyclically shifted by different offsets which are dependent on the block length 'Nb' and depicted in Table 2.

It is further continued using Mix Column Transformation.It is done by operating over different columns. In mix column transformation the columns of the current state are considered as polynomials of Galois Field (28). It is multiplied by modulo $x^4 + 1$ with a fixed polynomial

$$C(x) = [03]x3 + [01]x2 + [01]x + [02] \tag{2}$$

The decryption process is done by the reverse of encryption process i.e. Inverse Sub Byte, Inverse Shift Row Transformation, and Inverse Mix Column Transformation. Noticeably the Add Around Key operation is same as it perform the XOR operation, but the positions are reversed.

Table 1 Mapping of block length, key length and no. of rounds

Block length (bits)	Key length	No. of rounds
128	4	10
196	6	12
256	8	14

Table 2 Offset value of row shifting

Block length	Shift of row 1	Shift of row 2 (byte)	Shift of row 3 (byte)	Shift of row 3 (byte)
4	No change	1	2	3
6	No change	1	2	3
8	No change	1	3	4

Different types of hardware implementation has already made by different Researchers so far. CMOS based Rijndael Model [7] plays a great role in this area. But CMOSs face adverse effects from low power density, sub 10 nm physical limitations like problems. Then Jayanta and Prakash [8] attempted SET based Rijandael circuit. But it was a hypothetical approach only and also SET suffers from low current drive, background charge effect, lack of room temperature operable technology like troubles. So authors here have tried to make a Hybrid CMOS SET based Rijndael Model which compensates the drawbacks of CMOS and SET internally.

3 Hybrid CMOS Set Macromodelling of Rijndael Cryptography Technique

The authors adhered to PARTSIM simulator as the macro model of hybrid CMOS SET comprises of typical node applications. The node to node analysis is imperative for obtaining transient response and also it includes all the virtues of co tunneling phenomena within a Hybrid CMOS SET model. The versatility of PARTSIM is robustness, simplicity, easiness and above all it takes less computational time compared to other existing simulators.

Mohammad Reza Karimian et al., initiated the first macro modeling consisting of Quantizer to reinforce the SET tunneling phenomena [9]. Figure 1 depicts the proposed macro-model of the basic Hybrid CMOS SET inverter circuit using PARTSIM.

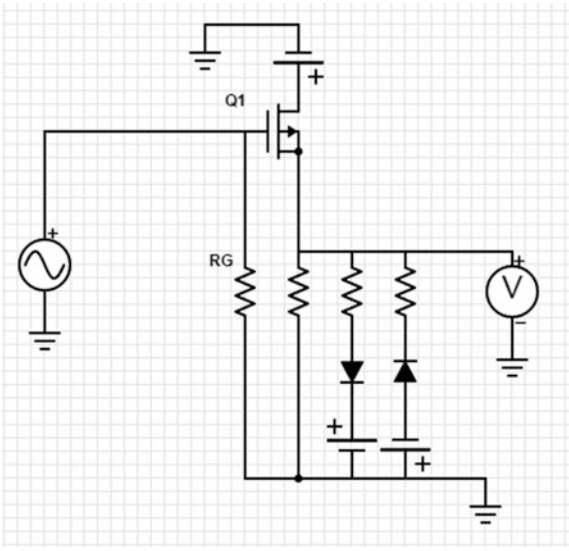

Fig. 1 Proposed macro-model of the basic Hybrid CMOS SET inverter circuit using PARTSIM

The Hybrid CMOS SET Affine Transformation module of Rijndael Cryptography Technique is demonstrated in Fig. 2, and the Inverse Affine Transformation module is followed next in Fig. 3 and subsequently both are simulated using PARTSIM.

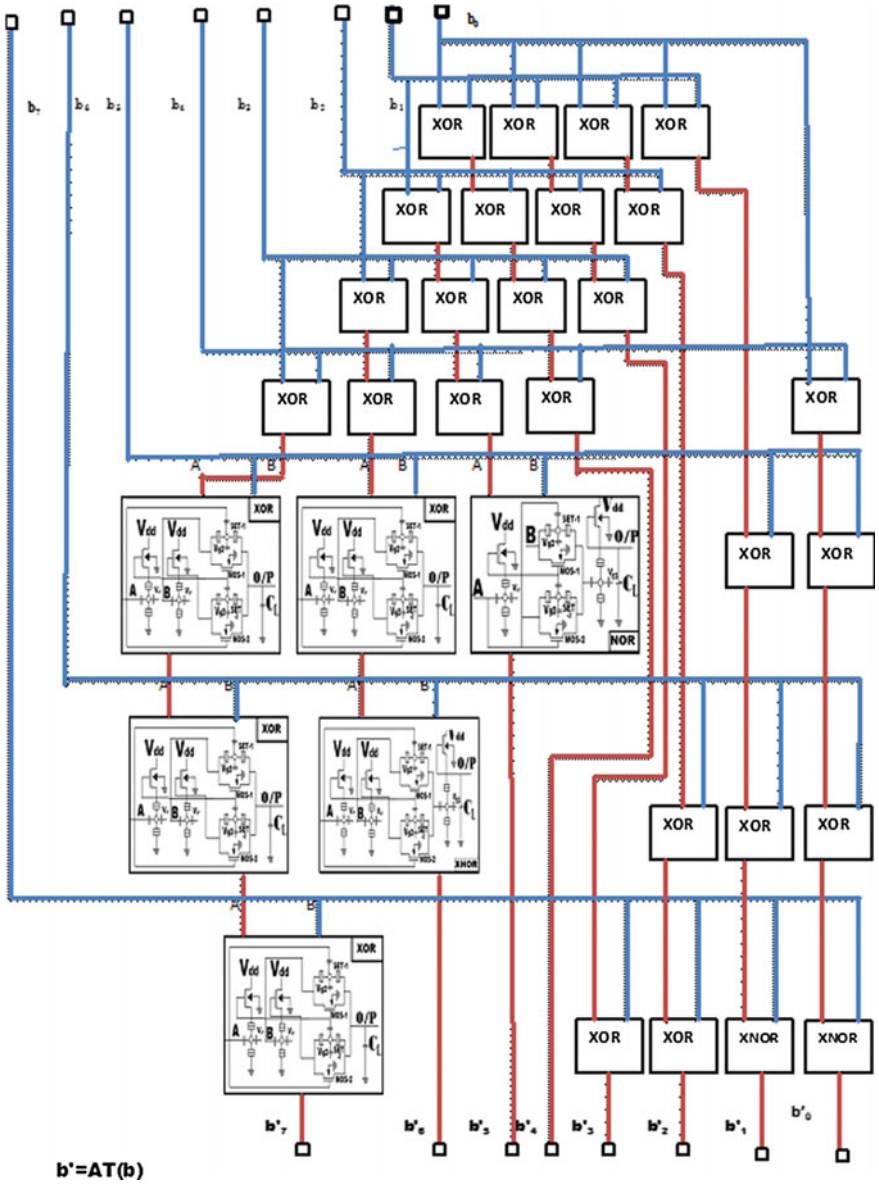

Fig. 2 The Hybrid CMOS SET Affine Transformation module

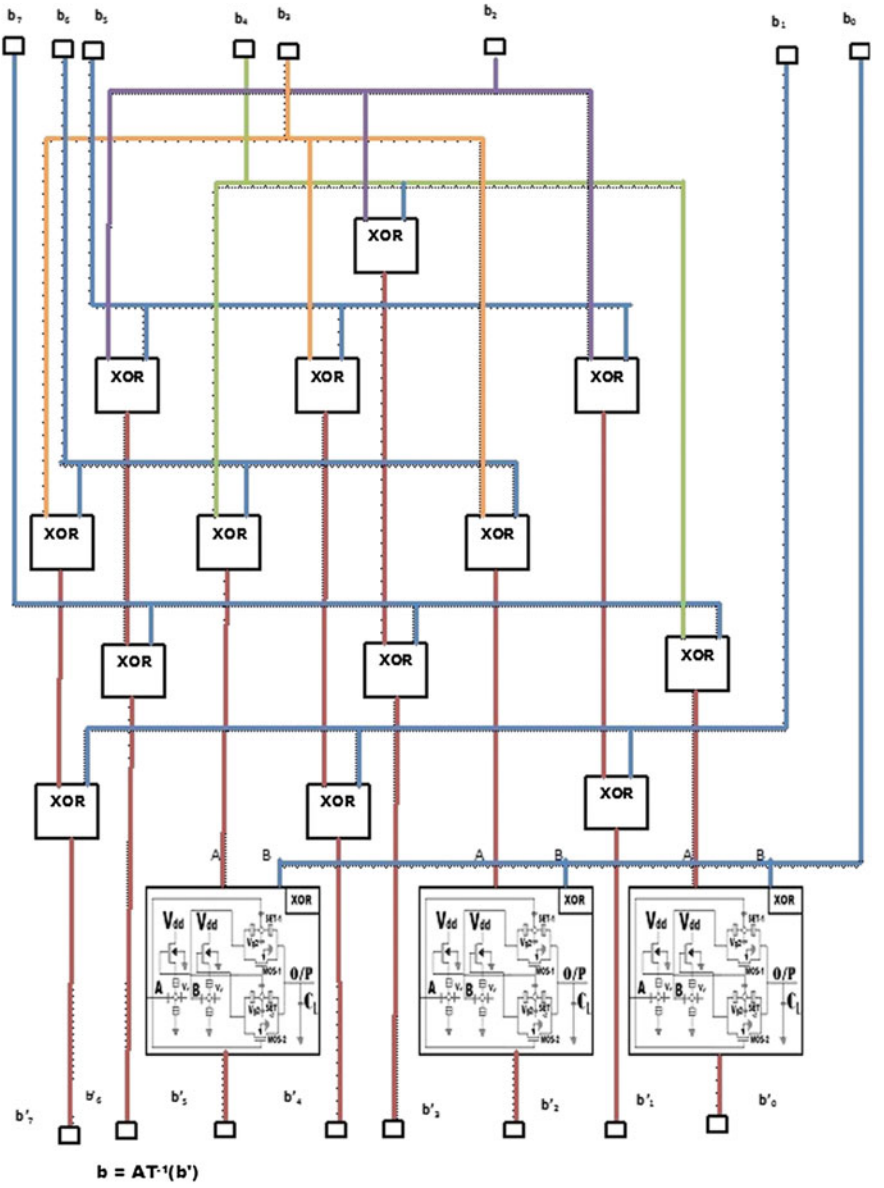

Fig. 3 The Hybrid CMOS SET Inverse Affine Transformation module

4 Conclusion

Simulation of both the structures reveal that the merits of Hybrid CMOS-SET modelling is finest and also high speed electron tunneling is omnipresent in both CMOS and SET part. It is a comprehensive ASIC designing of Rijandael Cryptography. The intrinsic Coulomb Blockade effect is controlled via exchange of regulated flow of electron supply from input V_{gs}. It is the ultimate form of device research where the authors can manipulate the flow of electrons. Empirical study aptly insights the goodliness of Hybrid CMOS SET compared to conventional CMOS. The offerings are limited to requirement of less number of gates compared to conventional CMOS Rijandael technique. As the number of gates are less so the propagation delay is also lessened which offers high speed. The integration density is also high and owing such high integrating density the circuit becomes non volatile. Furthermore, the typical aspirations of Rijandael is enunciated by true means. Thus the authors advocate for more Hybrid CMOS SET modellings in cryptography in near future.

References

1. Vinay Pratap Singh, et al., "Analytical Discussion of Single Electron Transistor (SET)," International journal of Soft Computing and Engineering (IJSCE). Papers 2(3), (2012).
2. Santanu Mahapatra, et.al., "Analytical modelling of Single Electron Transistor for Hybrid CMOS SET Analog IC Design," IEEE TRANSACTION ON ELECTRON DEVICE. Papers 51(11), (2004).
3. D. Samanta, S.K. Sarkar, "A simple SET-MOS universal hybrid circuit realization of all basic logic functions," IEEE Advances in Engineering, Science and Management (ICAESM), International Conference. Papers 336–339 (2012).
4. Dr. Reinhard Wobst, "The Advanced Enryption Standard (AES): The Successor of DES," Information Security Bulletine. Papers 31–40 (2001).
5. Prof. N. Penchalaiah et al. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)," International Journal on Computer Science and Engineering, Papers 02(05), 1641–1645 (2010).
6. J. Daemen and V. Rijmen, AES Proposal: Rijndael. Papers 2, (1999).
7. Joan Daemen and Vincent Rijmen, "A Specification for the AES Algorithm Rijndael," Papers 3 (7), (2003).
8. Jayanta Gope, Prakash Kumar Shah "Advanced and Secured Rijndael Hardware Realization Using Single Electron Transistor Technology," International Journal of Emerging Research in Management andTechnology, Papers 3(5), (2014).
9. Mohammad Reza Karimian et al., "A New SPICE Macro-model for the Simulation of Single Electron Circuits," Journal of the Korean Physical Society. Papers 56(4), 1202–1207 (2010).