*International Journal of Emerging Research in Management &Technology*
*ISSN: 2278-9359 (Volume-3, Issue-5)*
**Research Article** | **May 2014**

# Advanced and Secured Rijndael Hardware Realization Using Single Electron Transistor Technology

**Jayanta Gope*, Prakash Kumar Shah**
*Dept. of ECE,*
*Camellia School of Engg. &Tech. India*

***Abstract—***

***This document encompass the study of security issues connected with existing ATMs and other electronic fund transfer mechanism. As the matter of fact that hackers are committing uninterrupted crimes; thus emphasis is given here to use Rijndael algorithm for matured cryptography techniques in order to combat such unethical attempts. Few endeavours have been reported so far to design the Rijndael hardware that attracted researchers worldwide. But most of them are based on conventional CMOS technology. Here, our novel approach is to improvise the Rijndael using one highly advanced technology called Single Electron Transistor (SET) Technology which is one most dominating successor in post CMOS era. The attempt to model such huge design required through research in understanding the correlation of electron tunnelling between the junctions. A comparative study is conducted to reveal the underlying merits of SET based Rijndael model.***

***Keywords—Rijndael, S-BOX, Single Electron Transistor, Coulomb island, Tunnel Junction***

## I. INTRODUCTION

The Automated Teller Machines (ATM) introduced in 1939 has hit 1.5 million installations worldwide by the year 2005 [1]. This huge popularity of ATMs requires high integrated security to provide uninterrupted service to the users. The terminal's protection from unauthorized intruders is a next to impossible task, although banks do deploy highly skilled and armed security personnel in most ATMs. Thus, from the very inception, the personal identification number (PIN) provided by the banks to their customers has been of greater significance in the overall secured operation of ATMs. This is a kind of cryptography which is referred in banking operations or electronic fund transfer operations. Records of ATM attacks exposed the bare fact that the application of present day available cryptography in electronic fund transfer systems in all ATMs or electronic fund transfer operations is still insufficient as outbreaks can occur in different sub-systems at any time. More particularly, the safety of Electronic funds transfer terminals from attack by potential intruders physically and/or through electronic hacking is reported largely. In order to deal these problems, the banks now appreciate the combined implementation of physical security, procedural protection and adoption of advanced cryptography techniques.

One such predominant issues of cryptography techniques was largely necessitated in 1997 by US National Institute of Standards and Technology (NIST) and consequently the mostly accepted 'Rijndael' cryptography technique flourished as competent authority in October 2000 and then after it was announced as Advanced Encryption Standards (AES); it is further described as a new standard algorithm to combat attacks like exhaustive key search or exploiting the short key length of previous Data Encryption Standard (DES) [2]. Since then several hardware architectures for Rijndael were proposed and their performances were tested using ASIC libraries [3-5] and FPGAs [6-10]. Yet, very few of the circuit models are exactly according to the Rijndael specification although some of them have the possibility to be incorporated in near future for practical use. The AES undoubtedly needs to be embeddable not only in high-end servers but simultaneously in low-end consumer products like the mobile terminals. Consequently, sharing and reusing hardware resources, as well as compressing them to the logical synthesis are essential to produce a small Rijndael circuit.

Besides its theoretical and empirical studies using CMOS based IC realization; Researchers aimed to include it in various embedded consumable systems like Web Servers, ATMs, Fibre Distributed Data Interfaces (FDDIs), smart cards, cellular phones etc. As visualized that from the very dawn of 2000, numeral models for efficient VLSI realization of AES algorithm using ASIC libraries and FPGAs have been reported [11-16]. Achieving more precise integration or speed-up of such models using conventional CMOS technology was rather the most unattainable task. Although, research initiatives after mid 90s' changed its path and scaling down of silicon based CMOS technology became the basis of ITRS guided semiconductor industry as envisaged in all top scientific publications [17]. This scaling down was not an infinite process. Soon advanced device technologies that have greater functionality with small number of hardware components became indispensible for the future low power System-on-Chip (SoC) architectures. Reasonably the alternative search for new technologies like single electronics and quantum electronics acquired much interest.

Quantum electronics ushered high waves in designing ultra small electronic devices. The intrinsic merits of quantum device are (i) High speed and (ii) Small power dissipation. Such potentials make the Quantum devices the finest optimal for Very High-Speed Integrated Circuits (VHSIC), Ultra Large Scale Integrated (ULSI) Chips and for Wafer Scale Integration [18]. Then again the fragility of the quantum effects uncertain the future use of Quantum Electronics in VLSI

in the "More Than Moore" era. Some of the intrinsic limitations of Quantum devices that make these devices quite unpopular in present day small scale device technology are material and process related limitation, power limitation, wiring limitation, quantum mechanical limitation and system architecture limitation [19,20].

On the other hand Single-electron transistor (SET) rose up to be considered as one of the promising aspirants for future extremely-large-scale-integrated logic circuits owing to its ultra low power consumption and higher functionalities in low dimensional systems category. The elements of SET that attract most of the device Scientists and Engineers are - its small size, fast in action, and low power dissipation that increases the potentiality of SET made circuits for logic and memory operations [21, 22]. Single Electrons in other words is all about the controlled flow of electrons between small conducting islands [23]. It grew as a golden technology with new physical effects of charge transport. This transport phenomenon is of unmatched impetus as semiconductor device size is scaled down to continue with the exponential growth in density and performance, to sustain the Moore's law. Here, we have attempted to model a SET based Rijndael hardware architecture to cope up with next generation security systems. In the subsequent sections SET overview in very brief is given along with a short synopsis of Rijndael algorithm. It is followed by our proposed novel SET based Rijndael architecture and it concludes with a comparative study between our proposed SET based Rijndael model and previously attempted CMOS made Rijndael models.

## II. SINGLE ELECTRON TRANSISTOR - THE NEXT GENERATION TRANSISTORS

The increasing popularity of the SET technology remains 'unputdownable' because of the fact that charge transport occurs in discrete quantities, i.e., one electron at a time. This attributes the ability to design circuits in which the transport of individual electrons can be perfectly controlled. However, the most promising applications for SETs are (i) charge-sensing applications such as the readout of few electron memories, (ii) the readout of charge referred as coupled devices and (iii) precision charge measurement in metrology. The SET technology offers a wide range of advantages. First, it offers a greater scaling potential than CMOS as the device structure is less complex. Second, SET has the potential to realize circuits that consume much less energy than CMOS circuits. Third, recent advances in silicon based fabrication technology indicate that SET based circuits have the potential to operate at room temperature. Another advantage of the SET technology is that the tunnel junctions, the basic SET circuit element, can be fabricated in many different ways. Being so, today researchers are craze for designing low power consuming, nano-scaled, high integration density SET devices which will increase the device functionality much higher compared to present day CMOS made devices. Moreover, they are emphasizing in realizing fast switching, low power and less space consuming SET based logic circuits to substitute the conventional CMOS circuits as SET appears better candidate for the survival of the fittest in modern electronics [24-27].

### *A. Structure and Tunnelling of Electron in SET*

SETs are constructed by introducing two tunnel junctions in series [28-30]. The two tunnel junctions produce a "Coulomb Island" where electrons can only enter by tunnelling through one of the insulators. This device consists of three terminals much similar to that of a FET: i.e., both the outer face terminal of each section, and a "gate" terminal. The gate terminal is capacitatively coupled to the node between the two tunnel junctions. The capacitor appears like a third tunnel junction, but its thickness is more than the others restricting other electrons to tunnel through it. Basically the capacitor serves as a process of setting the electric charge on the Coulomb Island [31].

The tunnel junction structure consists of two pieces of metal. Both these metal plates are separated by a very thin (~1 nm) insulator similar to the figure shown in Fig.1. Electrons, in one of the metal electrodes can pass through or tunnel into the other electrode only through the insulator. In fact the tunnelling is a discrete phenomenon, the electric charge that flows through the tunnel junction flows in multiples of electrons. This electron is the charge of a single electron.

Elementary operations of tunnelling junction in SET are described in the Fig 2. For instance when an electron move toward 'A' and a pulse greater than 5mV is given i.e., if $\Phi_{n-1}$>5mV is applied, the electron is proficient enough to cross tunnel junctions (J1 and J3) to ('C' or 'E'). This tunnelling phenomena is subjected to the Coulomb energy [$E_c=e^2/(2C)$] + applied energy. Totalling of both these energies should be greater than the potential height of the barrier energy of junction(s) (J1 or J3). Subsequently, the electron tails the path 'QRST' or 'QRUV if the signal $X_i$>5mVand the corresponding total energy (i.e. Coulomb energy plus applied energy) is greater than static potential junction energy of J2 (or J4) [32]. For real time applications it is utmost necessary to design SET based various logic gates. Such SET based designs for NOR, XOR and XNOR gates are shown in Fig.3to5 respectively.

## III. RIJNDAEL ALGORITHM IN BRIEF

This cryptography technique is a byte-oriented symmetric block cipher. The amalgamation of a sequence of four primitive functions, Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-key are here executed round by round. The eminent quality of Rijndael is that it can support any key length and block length between 128 bits and 256 bits that are multiple of 32 bits independently. The number of algorithm that sequences round by round is denoted by 'Nr', and hangs on the message or key length. Proceeding to each round an Add-Round-key that combines the input with the cipher key is executed. The 'Key Expansion' algorithm spawns a key list for different rounds from the cipher key. Defining a 128-bit mode operation, at the beginning of the encryption, the message is divided to the blocks of length 128-bit and is then copied to a 16 byte rectangular array called 'State'. The Add-Round-key is nothing but a simplistic bit-wise XOR

operation in which the elements of the State are XOR-ed with Round-key bit-by-bit. The Sub-Bytes are considered as non-linear bit-wise substitution of all bytes in the State. In Sub-Bytes, apiece of every byte in the State is replaced by its corresponding byte in another table called 'S-Box'. The matured potential S-Box contains multiplicative inverse of all possible bytes over 'Galois field' denoted as $GF(2^8)$ monitored by an affine transformation. Each subsequent byte is a component of $GF(2^8)$ with higher order complex polynomial function given by $m(X) = X^8 + X^4 + X^3 + X + 1$. In the Shift-Rows transfer operation, each row of the state is deliberated independently and further the bytes in that row are at regular intervals shifted to the left side based upon the key-size of the algorithm under consideration. The pioneering factor is that for the $128^{th}$ bit key, the first row remains unmoved. On the other hand, following the first row the second, third, fourth….. rows are shifted one, two, three … bytes correspondingly.

The Mix-Columns conversion is a unique 'bricklayer' combination functioning on each column of the State. In Mix-Columns, every columns of the State are well thought-out as a 'four-term' polynomial over $GF(2^8)$; further they are multiplied with a constant valued or fixed polynomial $c(X) = \{03\}X^3 + \{01\}X^2 + \{01\}X + \{02\}$. Under a precise mathematical coordination the multiplications are performed in modulo $(x^4+1)$ manner. Simultaneously, the 'set of rules' for the decryption has the matching structure; but the proceedings are mathematical inverses of the encryption steps, i.e. Inverse-Sub-Bytes, Inverse-Shift-Rows, and Inverse-Mix-Columns. One fundamental aspect is that the round keys are the same as those in encryption however they are positioned in reverse order. Fig.6 is a sketch of the standard execution of the AES [33,34] using Rijndael.

## IV. HARDWARE REALIZATION OF RIJNDAEL CIRCUIT USING SET

The entire documentation of Rijndael was first encapsulated to design this painstaking model. The best methodology to implement SBOX is to decompose the polynomial Boolean function as described by eminent Scientist Sir Edwin NC Mui's in his research article entitled "Practical Implementation of AES SBOX" [35]. The SBOX table is represented as follows:

$$s(a) = \begin{bmatrix} a_7' \\ a_6' \\ a_5' \\ a_4' \\ a_3' \\ a_2' \\ a_1' \\ a_0' \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

And Inverse of SBOX is defined by:

$$s^{-1}(a) = \begin{bmatrix} a_7' \\ a_6' \\ a_5' \\ a_4' \\ a_3' \\ a_2' \\ a_1' \\ a_0' \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Here 'a' is the value of original number which is under consideration; 'b' denotes the multiplicative inverse of 'a`' and 'b`' is the end result of SBOX substitution. In addition, the function s(a) is the operation of finding SBOX substitution of 'a' whereas $s^{-1}(a)$ is operation of finding the inverse SBOX of 'a'. The reason behind such consequences is that the matrix multiplication can be easily implemented on Logic gates, although one problem to obtain the multiplicative inverse of $GF(2^8)$. The solutions are the modules defined as:

1) Affine Transformation Module
2) Inverse Affine Transformation Module
3) Isomorphic Mapping Module
4) Inverse Isomorphic Mapping Module
5) $GF(2^4)$ Squarer Module
6) $GF(2^4)$ Lambda Multiplication Module
7) $GF(2^4)$ Multiplicative Inverse Generator Module
8) $GF(2^4)$ Multiplication Module

Due to shortage of space authors here confine themselves into Affine Transformation Module and Inverse Affine Transformation Module. The SET based gates are positioned in a manner to obtain the minimum contact area plus through consideration is given in maintaining higher integrity level; moreover the sophistication but simplicity was given the first priority during circuit modelling

The first circuit shown in Fig.7 denotes the SET based Affine Transformation Module which is followed by the Inverse Affine Transformation Module given in Fig.8. The modus operandi of this circuit although is fascinating but the logic behind its operation is kept low profile to avoid designing fragility; simultaneously the circuit becomes effective and has less propagation delay. Besides, the integration density of the novel architecture increases and the heat dissipation reduces considerably. The tunnelling of electrons in both the circuits is the matter of concentration. The experiential design is further made ready for Monte Carlo based simulation platform. The outcomes acquired are of better appropriateness and the process has greater proximity in being realized in an on-chip platform. Detailed analysis of the circuit is avoided here due to space limitations but the vital statistics are laid down in the following sections to study its effectiveness in the post CMOS era.

*A. CMOS Rijndael vs. SET Rijndael*

The proposed modelling of SET based Rijndael IC largely showed enormous robustness in transient analysis test using Monte Carlo based simulation settings for its maximum exploitation. The proposed modelling of this SET based system considerably reduces power consumption; its efficient design structure increases the integrity of the IC which is quite sufficient to provide output at a quicker speed. Accordingly, the most desired very high-speed computation is attained with this newly proposed SET configuration. The power dissipation for switching a single bit is of few µW which is extensively lesser when compared to conventional CMOS devices Rijndael circuits. With such unmatched distinguishing merits, the SET based Rijndael IC designed shows tremendous prospect of providing much more component density thereby reducing the future IC sizes. Besides, all other phenomenal individuality of SET circuit the model reflects its robustness than any conventional CMOS based circuit.

## V. CONCLUSIONS

The detailed comparative study reveals that SET based Rijndael circuit posses less propagation delay of about 6ns/gate which is nearly half of CMOS based design. Similarly the power dissipation/gate using SET is reduced to lowest as ~1µW approximately 10 to 12 times lower than conventional CMOS architectures. Further dealing with power consumption it clearly distinguishes that SET based Rijndael consumes only $1/10^3$ times power per gate than CMOS made models. Whereas the fastness doubles for SET made circuits. These empirical results signify that the Single Electron technology which is the basis of next generation Rijndael exact modeling is built on the robust effects of the electronic charge discreteness. The most unique feature is that the composite structure of SET has an immense size reduction possibility which in turn increases its integrity. Here emphasis is given to see that single charge is efficiently incorporated to manipulate and control the correlated electron tunneling in small capacitance structure. Further the logical combinations create appreciations in future SET based logic circuits.

Modern era that demands highly secured but non complex and less time consuming efficient electronic fund transfer mechanism or un-hack-able ATMs is anticipated to rely on such SET based Rijndael models. The proximity to incorporate such models lies very close to the line of reality. Thus in this scenario SET technology stands much ahead when compared to conventional electronics.

## ACKNOWLEDGMENT

We hereby acknowledge the kind technological and financial support provided by Prof. (Dr.) A. S. Chaudhury, Hon'ble Director of Camellia School of Engineering and Technology, West Bengal, India, to carry out this rigorous research.

## REFERENCES

[1] 'Number of ATMs worldwide expected to hit 1.5 million in December 2005' www.atmmarketplace.com article.
[2] Daemen, J, and Rijmen, V.: AES Proposal Rijndael, National Institute of Standards and Technology, July 2001.
[3] T. Ichikawa, T. Kasuya, and M. Matsui, "Hardware Evaluation of the AES Finalists", The Third Advanced Encryption Standard Candidate Conference, pages 279–285. NIST, April 2000.
[4] B. Weeks, M. Bean, T. Rozylowicz, and C. Ficke, "Hardware Performance Simulation of Round 2 Advanced Encryption Standard Algorithm", available at http://csrc.nist.gov /encryption/aes/round2/NSA-AESfinalreport.pdf.
[5] T. Ichikawa, T. Tokita, and M. Matsui, "On Hardware Implementation of 128-bit Block Ciphers (III)". In2001 Symposium on Cryptography and Information Security (SCIS 2001), pages 669–674, January 2001.
[6] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists" The Third Advanced Encryption Standard Candidate Conference, pages 13–27. NIST, April 2000.
[7] N. Weaver and J. Wawrzynek, "A Comparison of the AES Candidates Amenability to FPGA Implementation" The Third Advanced Encryption Standard Candidate Conference, pages 28–39. NIST, April 2000.
[8] K. Gaj and P. Chodowiec, "Comparison of the Hardware Performance of the AES Candidates using Reconfigurable Hardware" The Third Advanced Encryption Standard Candidate Conference, pages 40–56. NIST, April 2000.
[9] M. McLoone and J.V. McCanny, "High performance Single-chip FPGA Rijndael Algorithm Implementations" Workshop on Cryptographic Hardware and Embedded Systems (CHES2001), pages 68–80, May 2001.
[10] V. Fischer and M. Drutarovsky, " Two Methods of Rijndael Implementation in Reconfigurable Hardware" Workshop on Cryptographic Hardware and Embedded Systems (CHES2001), pages 81–96, May 2001.
[11] Fischer, V, and Drutarovsky, M, "Two Methods of Rijndael Implementation in Reconfigurable Hardware" Proc. CHES, Paris, France (2001) 77-92
[12] Sklavos, N, and Koufopavlou, O., "Architectures and VLSI Implementation of the AES Proposal Rijndael" IEEE Trans Computers, 51, 12 (2002) 1454-59
[13] Lu, C, C, and Tseng Y, S., "Integrated Design of AES (Advanced Encryption Standard) Encryptor and Decryptor", in Proc. IEEE Int. Conf. Application Specific Systems, Architectures Processors (2002) 277-285
[14] Satoh, A, Morioka, S, Takano, K, and Munetoh, S., "A Compact Rijndael Hardware Architecture S-BOX Optimization", in Proc. ASIACRYPT 2001, Gold Coast, Australia (2000) 239-254

[15] Zhang, X, and Parhi, K,K., "Implementation Approaches for the Advanced Encryption Standard Algorithm", IEEE Circuits Mag., 2, 4 (2002) 24-46
[16] Zhang, X, and Parhi, K, K., "High-Speed VLSI Architectures for the AES Algorithm", IEEE Trans. Very Large Scale Integration (VLSI) Systems, 12, 9 (2004) 957-967
[17] Fortes, J., "Future challenges in VLSI System Design", Proceedings IEEE Computer Society Annual Symposium on VLSI (ISVLSI'03) (2003) 5-7.
[18] Peter W. Hawkes "*Advances in Electronics and Electron Physics*", Volume 89, ACADEMIC PRESS, 1994.
[19] K.K. Berggren, "Quantum computing with superconductors," Proceedings of the IEEE, pgs. 1630 – 1638, Oct. 2004
[20] A. Narayanan, "Quantum computing for beginners," Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on, 6-9, pgs. 2238 Vol. 3, July 1999
[21] K.K. Likharev, "Correlated discrete transfer of single electrons in ultra small tunnel junctions", *IBM J. Res. Devel*., vol. 32, pp. 144-158, January 1988.
[22] Casper Lageweg et al "Single-electron encoded latches and flip-flops" – IEEE trans. On nanotechnology, vol.3, no.2, June 2004
[23] Yukinori Ono, Yasuo et.al., "Fabrication Method for IC-Oriented Si Single-Electron Transistors" IEEE TRANSACTIONS ON ELECTRON DEVICES, VOL. 47, NO. 1, JANUARY 2000
[24] Jayanta Gope, et.al., "Single Electron Device Based Application Specific Integrated Circuit Design for Use in Stock Market" In National Conference on Advanced Computing and Computer Networks (NCACCN 2007), Vikhe Patil College of Engineering, Ahmednagar, Maharasthtra on 9-10 March 2007.
[25] Jayanta Gope, et.al. "Single electron device based string detector for the identification of Frame Delimiters in Data Transfer Protocols", National Conference on Digital Information Management (NCDIM'07), Thadomal Shahani Engineering College & Computer society of India, Mumbai-400050, during 23-24th March 2007.
[26] Jayanta Gope, et.al. "Single Electron Device Based Tea Vending Machine", International Engineering and Technology (IETECH) Journal of Information Systems, Vol-2; No:2, 2008, pp 046-051.
[27] Jayanta Gope, et.al., "Cellular Automata Based Data Security Scheme in Computer Network using Single Electron Device" Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010
[28] Liddle, David E., "The Wider Impact of Moore's Law", Solid State Circuits Newsletter. IEEE, September 2006
[29] H. Iwai et al., Microelectronic Engineering 28, pp. 147-154, 1995
[30] Y. Ochiai et al., , Microelectronic Engineering 30, pp. 415-418, 1996
[31] Khanna V.K, "Physics of carrier-transport mechanisms and ultra-small scale phenomena for theoretical modelling of nanometer MOS transistors from diffusive to ballistic regimes of operation" Phys Rep, pp 67–131, 2004
[32] W. Zheng, J.R. Friedman, D.V. Averin, S. Han, and J. Lukens, "Coulomb Blockade and Universal Scaling in Resistively Isolated Tunnel Junctions", Report at the APS March Meeting Los Angeles, March 1998.
[33] Daemen, J, and Rijmen, V.: The Design of Rijndael, Springer (2002)
[34] Rijmen, V, Efficient Implementation of Rijndael S-Box, available online at: www.iaik.tugraz.at/research/krypto/AES/old/~rijmen/rijndael/sbox.pdf
[35] Edwin NC Mui, "Practical Implementation of Rijndael S-BoxUsing Combinational Logic", Custom R&D Engineer Texco Enterprise Pvt.Ltd

## LIST OF FIGURES

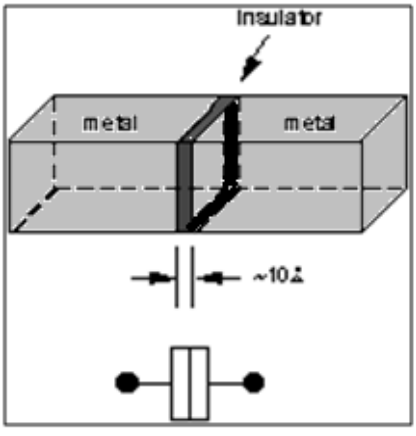


Fig. 1 Schematic Diagram of Tunnel Junction

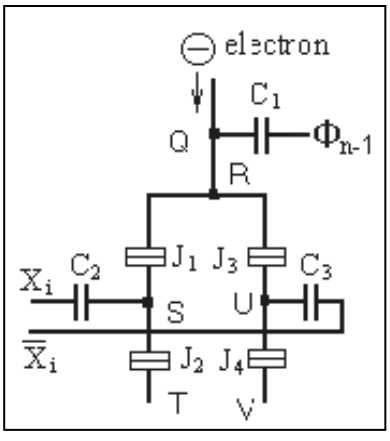


Fig. 2 Basic operation of Tunnelling Junction

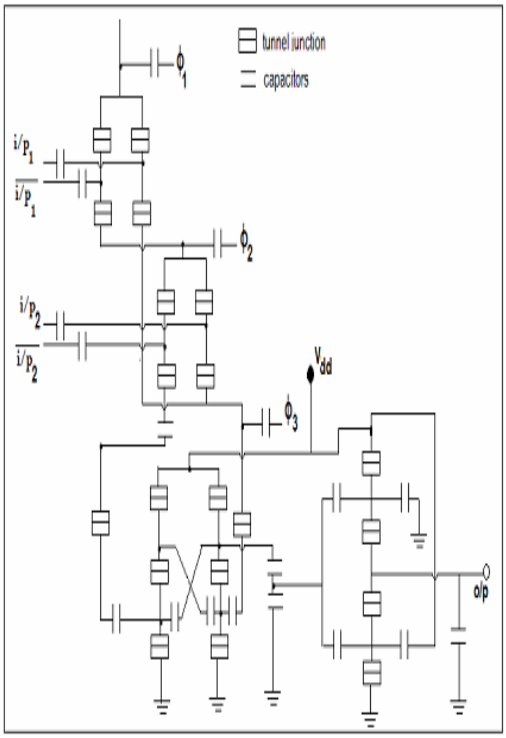


Fig. 3. SET based NOR gate

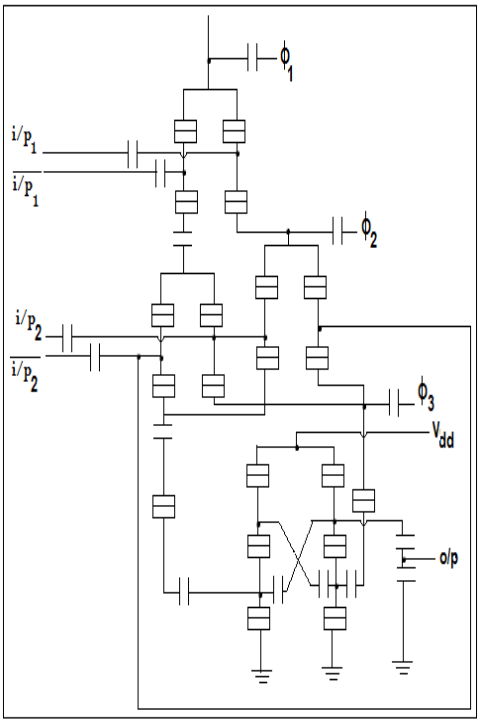


Fig. 4 SET based XOR gate

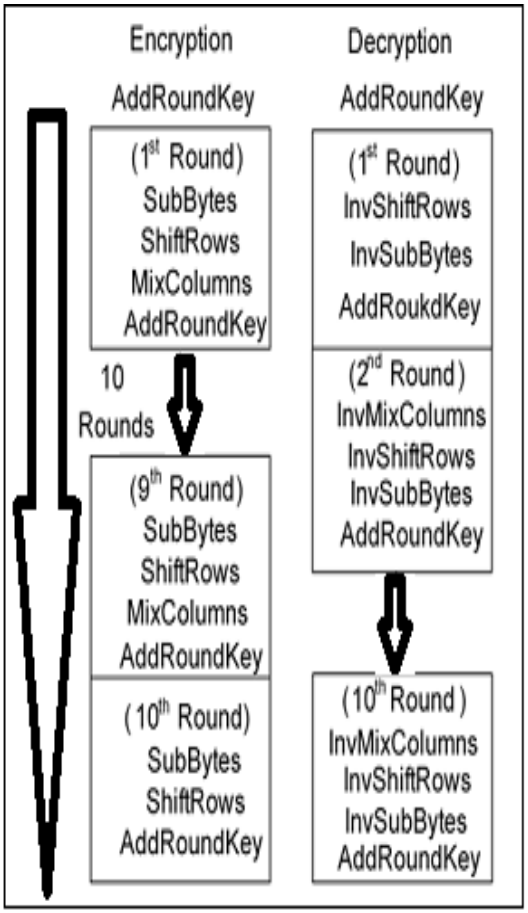


Fig. 5.SET based XNOR gate

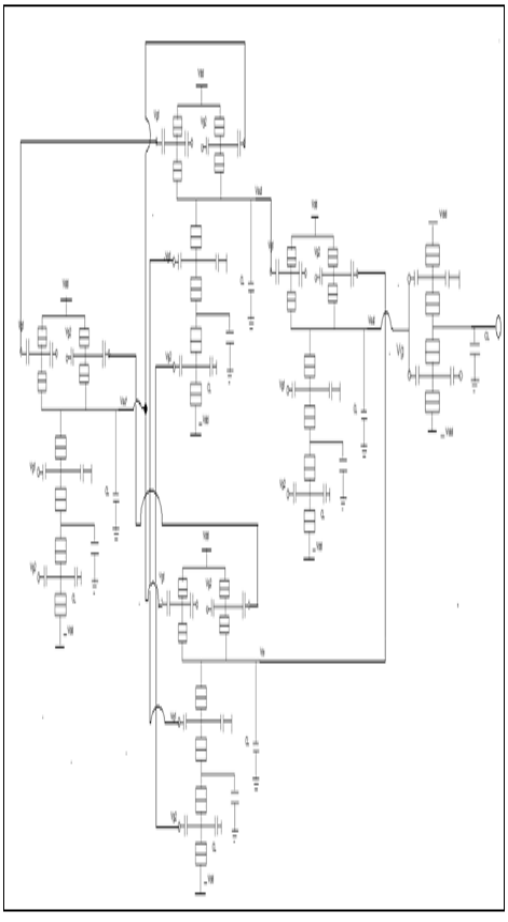

Fig. 6 Rijndael Algorithm in block

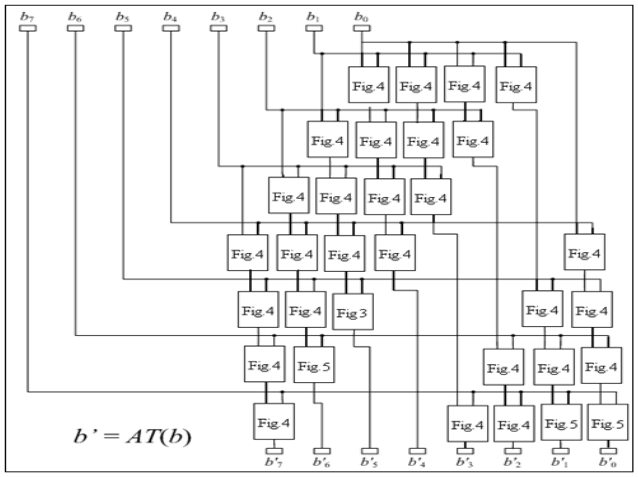


Fig. 7 SET based Affine Transformation Module

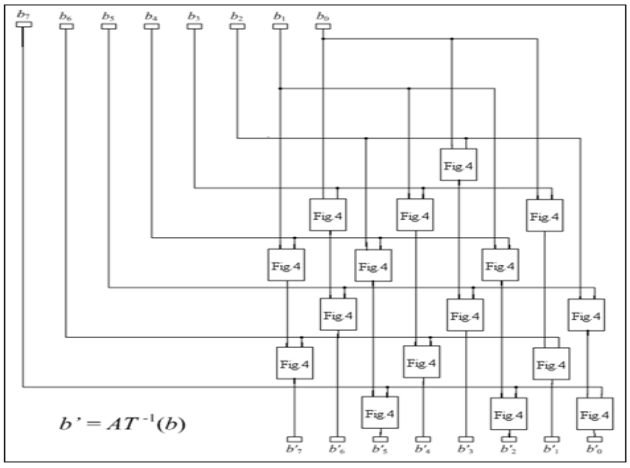


Fig. 7 SET based Inverse Affine Transformation Module