A modernistic architecture of masked Advanced Encryption Standard algorithm for SAN

Vasantha Kumara S[1], Dr.Indumathi T S[2]

[1]Department of Digital Electronics and Communication Systems, Visvesvaraya Institute of Advanced Technology, Muddenahalli, Chikkaballapur, India

[2]PG Co-ordinator, Visvesvaraya Institute of Advanced Technology, Muddenahalli, Chikkaballapur, India

***Abstract* - The present information and technology processed by computers to access the private information like video conferencing, account status in bank, e – transaction of money and business deals through internet for all these encryption of the information in various forms are necessary. So to protect the information from different attacks using symmetric or asymmetric key encryption by adding the random value to the intermediate result is called masking. In terms of computational complexity symmetric key algorithm is less complex than the asymmetric or multiple key algorithms. The aim is to provide the data security to the storage area network and also the proposed method is to optimize the masked AES with the unrolled structure and it can be achieved through mapping operation. Hence to optimize the area of masked AES only needs to map the plain text and masking values from Galois Field 256 (GF (2^8)) to Galois Field 16 (GF(2^4)) once at the start of the operation and map the cipher text back from Galois Field 16 to Galois Field 256 once at the end of the operation. So just moving masking operation as well as the inverse mapping operation outside the masked advanced encryption standard algorithm round function area can be reduced.**

***Index terms* – AES, SAN, Galois Field, Masking.**

I. INTRODUCTION

The sensitive data stored in the data network or in the storage area network involves the risk leakage of information in embedded application. With the worldwide communication of private and confidential data over the storage area networks or the internet, there is always a possibility of threat to data confidentiality, data integrity and data availability. Data encryption maintains data confidentiality, integrity and authentication. Information has become of the most important assets in growing demand of need to store every single importance of events in everyday life. Messages need to be secured from unauthorized party. Encipherment is one of the security mechanisms to protect information from public access. Encryption hides the original content of a message so as to make it unreadable to anyone, except the person who has the special knowledge to read it.[2]

Masking, as an anti-DPA strategy, is widely used. In a reliable masked encryption scheme, all possible values of an internal node are randomized and mapped to the same distribution, and the power consumption is no longer dependent on the original internal value. There are two types of Masking Multiplicative Masking and Boolean Masking both are used to avoid the correlation between the power consumption and the secret keys[3]. Multiplicative masking is realized through either standard CMOS cells at gate level or nonstandard CMOS cells where as Boolean masking can be realized at algorithmic level and is resist to differential power analysis and glitch attacks. The Boolean masking is good to implementation because there is no need of extra hardware.[1]

In this paper various techniques are developed to reduced the area of a masked AES for Storage Area Networks. The proposed masked AES mainly perform over Galois Field 16 (GF(2^4)), and the related operations like the masked Shift Rows , masked sub bytes , masked Mix Columns, masked Add Round Key, and also for decryption inverse shift rows, inverse sub bytes , inverse mix columns and add round key including redundant masking values are all calculated over Galois Field 16(GF(2^4)).

II. PREVIOUS WORKS

In the past cryptography the encryption and decryption had done using confidential secret keys. But now a day's cryptography is defined in different mechanisms like asymmetric –key encipherment (called as public key cryptography) and symmetric key encipherment (called as private key cryptography). For a public key the computation time is high and also it's algorithm is complex. The private key have only one key for encryption as well as the decryption where as public key involves two keys each for encryption and decryption. There are many cryptographic algorithms such as Elliptic Curve Cryptography (ECC), Data Encryption Standard (DES), 2- DES, 3- DES, the Advanced Encryption Standard (AES) and other algorithms. But many hackers and investigators are trying to break algorithms through brute force and side channel attacks. Some hackers

ISSN: 2278 – 7798

successful in the case of Data Encryption Standard (DES) in 1993.[6]

The Advanced Encryption Standard (AES) is considered as one of the strongest published cryptographic algorithms. AES is a standard symmetric block cipher which successfully replaces the older data encryption standard (DES) as the approved standard for large number of application. The older 3DES was too slow and also supports only 64 bit block size. Then NIST (National Institute of Standard and Technology) searched for high efficient, highly secured and large key size supportable algorithm. All above condition and functions successfully satisfied by AES algorithm which is highly efficient good security strength supports up to 128, 192 and 256 bits key length. NIST finally selected Rijindael algorithm out of all algorithms that were submitted. The rijindael pronounced as **"rain doll"** developed by Dr. Joan Daemen and Dr. Vincent Rijmen both cryptographers from Belgium.[8]

Mainly three categories of criteria used by the NIST to select any algorithm they are:

a) Security: Resistance to cryptanalysis, soundness of mathematics, randomness of output, etc
b) Cost: Computational effiency nothing but speed, Memory requirements.
c) Implementation Characteristics/ Algorithm: Flexibility, Hardware and software suitability, and algorithm simplicity.

Kocher was first broke the AES by means of power analysis attacks. Power analysis attacks are simple power analysis attacks (SPA), differential power analysis attacks (DPA), higher order differential power analysis attacks(HODPA) and Glitch attacks. From then on, various methods has been developed to countermeasures for the AES implementation against power analysis attacks.

III. PROPOSED MASKED AES FOR UNROLLED STRUCTURE

For securing the information transformation the secure approach is cryptography. Power analysis attacks constitute a major threat to implementation of cryptographic algorithm. Different types of the power analysis attacks are glitch attack, higher order differential power analysis (HODPA), differential power analysis attack (DPA), simple power analysis attack (SPA). In SPA the attacker directly view the power consumption of the system. This power variation is based on the instruction performance. A SPA attack primarily depends on identifying of relevant power function. SPA analysis can, for example in DES implementation is revealing the difference between the multiplication operation, etc. Differential power analysis attack is much more strong attack than the SPA. The DPA use the error correction technique and statically analysis to extract data correlated to secret keys[9]. The implementation of DPA can done two phases such as data collection and data analysis. The higher order differential power analysis attacks (HODPA) used to correlate information in multiple cryptographic sub operation. DPA attacks introduce to address or miss vulnerabilities to the higher order DPA attack. The Higher order DPA attack can be recognised by collecting the signal from multiple resources, different measuring technique and different temporal offsets that are combined during application of DPA technique. The glitch attack is nothing but the postponing the input signal through circuit using different arrival time at gate level.

So various methods have been discovered to resist against above power analysis attacks. Masking is one of the very popularly used techniques which have low cost and easy implementation. The common approach to protect the information transformation in the AES against the differential power analysis attacks the input data given to the AES randomize the intermediate results that present in the computation of the algorithm. The approach by adding the random value to the intermediate result is called the masking.

A. MASKED AES

In masked AES the Boolean masking implementation is done because it has the advantage of easy implementation. In the exclusive oring with the random mask m. In the round function of AES Shiftrows, Mixcolumns, and AddRoundKEYs are the linear transformation but the SubBytes is the non-linear transformation of the AES.[11]

The linear transformation is defined as oper, then the masked oper can be written as the oper($x \oplus m$) = oper (x) $\oplus$ oper (m). But the subByte is non linear transformation for this the SubByte has the characteristic as S–box($x \oplus m$) $\neq$ s-box(x) $\oplus$ s-box(m). In order to mask the non linear the new s-box is denoted and is defined as s-box'. Further it can recomputed as s-box'$(x \oplus m) = s - box(x) \oplus m'$, where m and m' are the input and output masks of subBytes . The masking of 128 bit AES, it usually needs 6 byte random values such as m, m', m_1, m_2, m_3 and m_4. These six random values defined as $m_{1234} = \{m_1, m_2, m_3, m_4\}$ as the mask for one 32 – bit Mixcoloumn transformation and it also holds that m'_{1234}= Mixcolumn(m_{1234}) . Masked Mixcolumn can be scaled to adjust the operation over the GF(2^4) and it needs to deduce the scaling factor of a modular multiplication with the fixed co- effients 0X02 and 0X03.

The field GF(2^8) is an extension of the field GF(2^4). To perform the modular reduction requires an irreducible polynomial degree 2, $X^2 + X + \{e\}$, and another irreducible polynomial of degree 4, $X^4 + X + 1$. In order to reduce the hardware resources masked AES engine mainly calculated over GF(2^4). Figure 1(a) shows the proposed masked AES which moves the mapping and inverse mapping outside the AES's round functions. The plaintext and the masking values are mapped once from the GF (2^4) to the original field GF(2^8). In the brief all the masking values need to be mapped from GF (2^8) to GF (2^4) and we denote m_{84} = map(m), m'_{84} = map(m'), $m_{1234\ 84}$ = map(m_{1234}) , and $m'_{1234\ 84}$ = map(m'_{1234}).

ISSN: 2278 – 7798

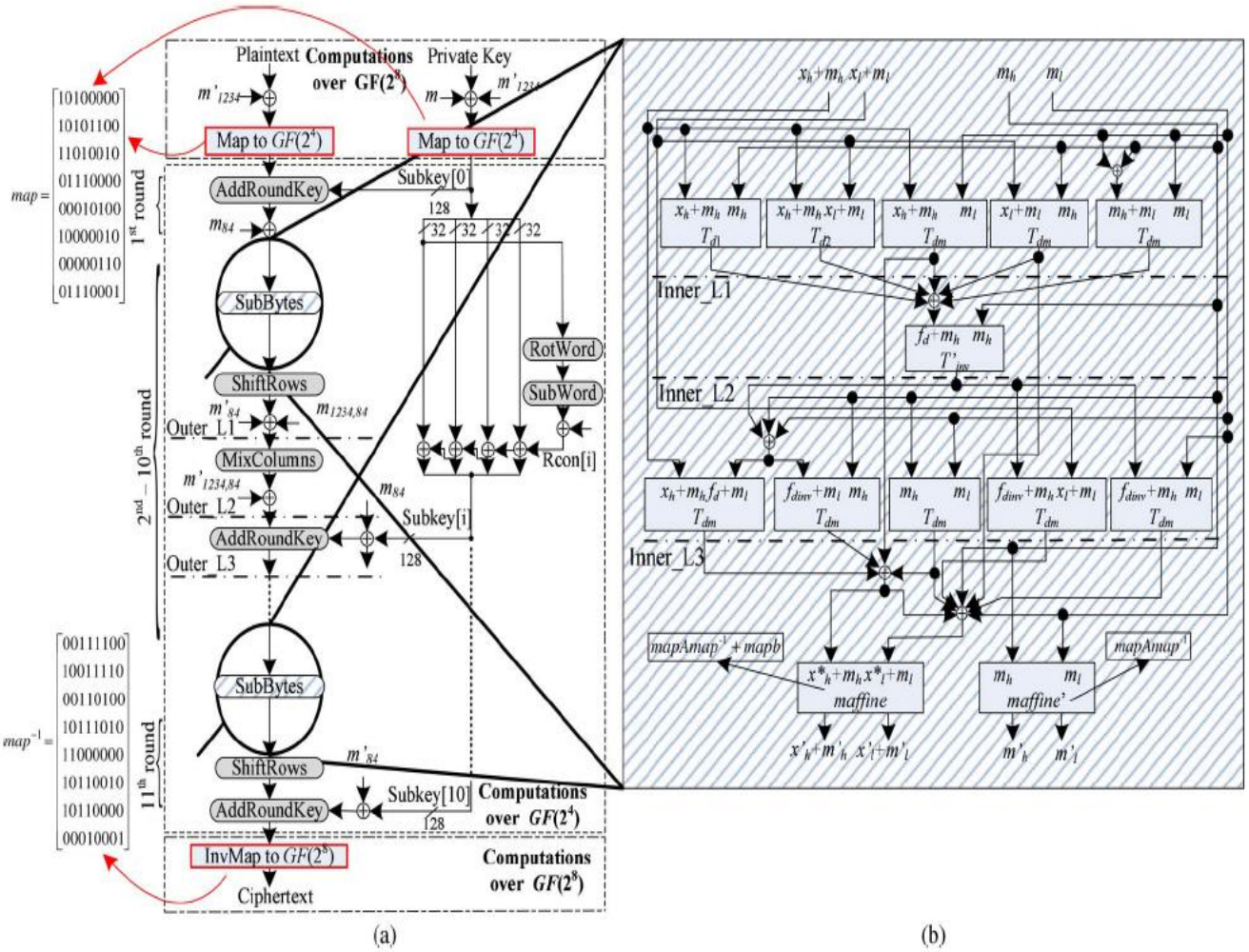

Figure 1 (a) Masked AES 1 (b) Masked S-BOX

The figure 2 shows the architecture of key generation module w1,w2,w3, w4 are the keys of the round. Rot word () means the cyclic shift of one byte. Sub word () means byte substitution and Rcon () is the constnt of the corresponding XOR operation of the N^{th} round encryption.[11]

B. PROPOSED ARCHITECTURE OF MASKED S – BOX

Masking countermeasure aganist power analysis attacks based on secret sharing. It decreases the correlation between the power consumed by device and the data being processed by applying random mask to the intermediate values. More formally, prior to the execution of the algorithm, the secret key value (or the input data value or both of them) x is obscured using the random value m, called mask , to generate a masked value x'. Figure 1(b) shows the map operation of masked s – box. In order to move the mapping and inverse mapping outside AES round operation we exchange the computational sequence of masked s – box. The masked affine and inverse mapping function with in the masked s – box. The masked affine function needs to be adjust with the new scaling factors.

The map operation is the mapping transformation of 8 X 8 matrix and map^{-1} is constructed by inverse map operation. Consider the input values of map are (z + m) and m, output values are (z + m)' and m' where {(z + m), m}€ $GF(2^8)$ and {(z + m)' , m'}€ $GF(2^4)$ and it holds[12]

((z + m) +m)' = map((z + m)+ m)----------(1)

The needed six precompiled table for implementing masked s- box over GF (2^4) are

1. T_{d1}: ((x + m),m) → x^2 X e +m.
2. T_{d2}: ((x + m)(y + m')) → ((x + m) + (y + m') X (y + m').
3. T_{dm}: ((x + m), (y + m')) → (x + m) X (y + m')
4. T'_{inv}: ((x + m), m) → T_{inv} (x) + m.
5. T'_{map}: ((x + m), m) → T_{map}(x + m)
6. $T'_{map^{-1}}$: ((x + m), m) → T_{map}^{-1}(x + m)

The (z + m)' = { $a^*_h + m_h$, $a^*_l + m_l$} and m' = {m_h, m_l}, maffine and maffine' are need for scaling the output masking values. Figure 3 shows affine function from $GF(2^8)$

ISSN: 2278 – 7798

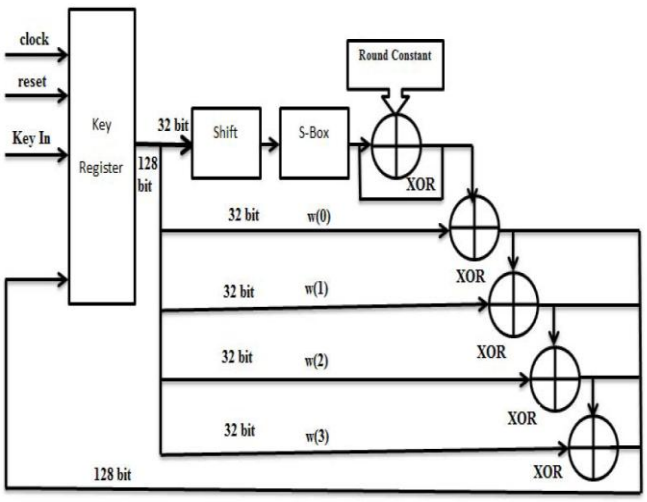

Fig 2 architecture of key generation module.

to GF (2^4). The normal affine function (Ax + b) is applied to the equation 1

A ((z + m) +m) + b = A map^{-1}((z + m)+ m)'+ b -------(2)

When mapping the equation 4.2 GF (2^8) to GF (2^4) then

Map(A(z +m) + b) + map Am = map (A map^{-1}(z +m +m)' +b) ----------(3).

Map(A (z+ m)+ b) + map Am = mapA map^{-1}(z + m)' + map b + mapA map^{-1}m'----(4)

Therefore we deduce that
maffine = mapA map^{-1} + map b and maffine' = mapAmap^{-1}

IV. RESULTS

In the Encryption step, a key of length 128 bit is used to encrypt an input data (data to be encrypted) of length 128 bit as shown in figure 3. The proposed masked AES algorithm takes 10 rounds to encrypt the data. Each round has four steps.

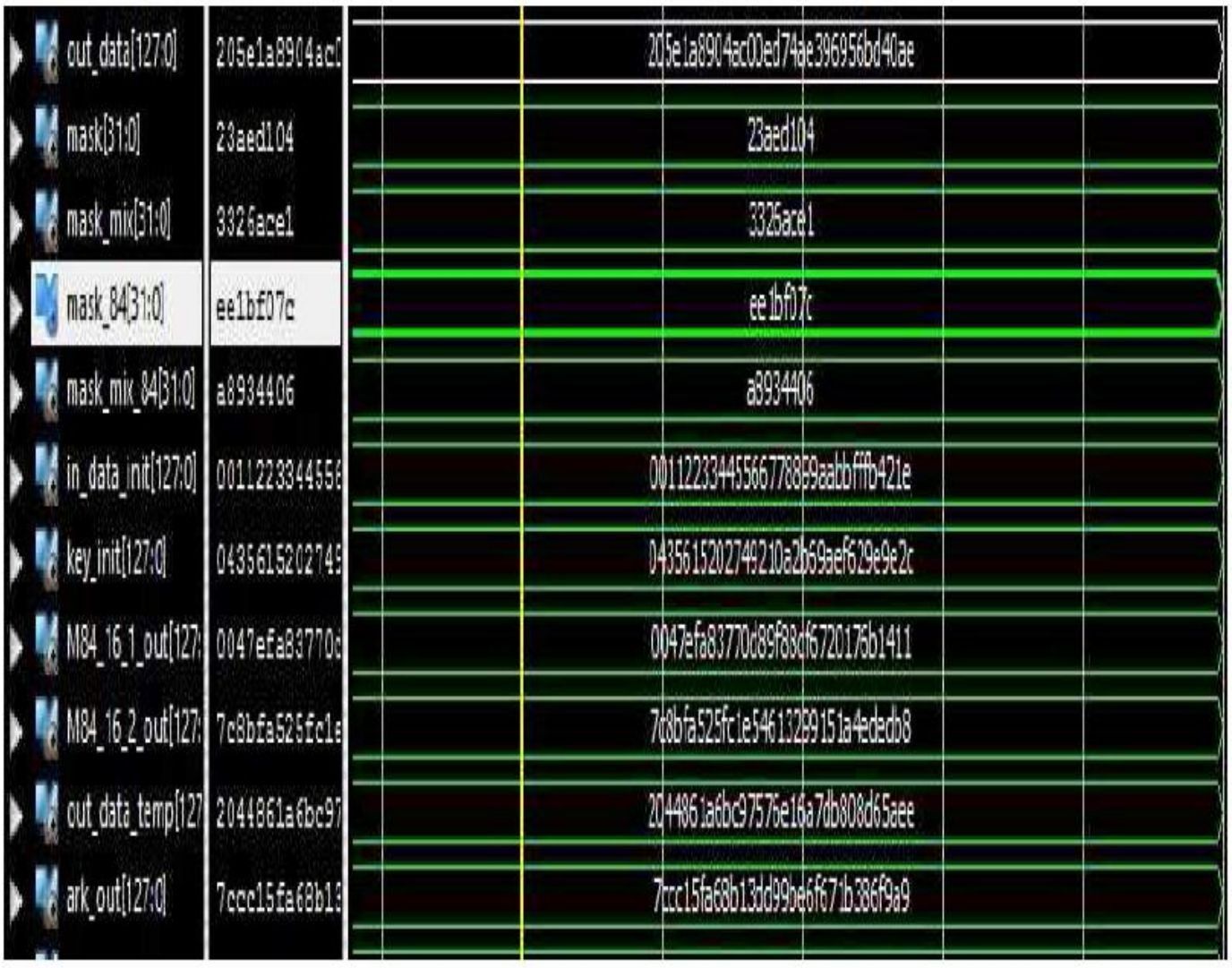

Figure 3 Encrypted outpu

ISSN: 2278 – 7798

1) Substitute bytes,
2) Shift rows,
3) Mix columns, and
4) Add round key.

After the completion of each round, a 32 bit key is used to mask the encrypted data. Simulated values are as follows.

128 bit input: = 00112233445566778899aabbccddeeff

128 bit Key: = h0435615202749210A2B69AEF51B832CD

Encrypted output after masking:
205e1a8904ac00ed74ae396956bd40ae.

V. CONCLUSION

In this paper for protecting data at rest in the storage area network we proposed the optimized area efficient masked AES with 32 – bit and 128 – bit data path (masked s – box over the GF(2^4)) separately. Here the masked AES only needs map the plain text and masking values from GF(2^8) to GF(2^4). Once at the beginning of the operation and map the cipher text back from GF(2^4) to GF (2^8) once at the end of the operation. Therefore by moving the mapping and inverse mapping outside the masked AES's round function area can e reduced. Compared with a state-of-the-art design, our implementation reduces the overall area by 36.2% (20.5% is contributed by the main method, and 15.7% is contributed by the BRAM optimization).

In feature we can optimize the S- box over the Galois field GF (2^2) in which the optimization of area of the masked AES reduced and with less memory masked AES can generate but it's mapping becomes more complex. Instead of 128 bit key use the 256 bit key for masked advanced encryption and which involves 14 round of computation and it quite difficult.

REFERENCE

[1] Yi Wang and Yajun Ha, Senior Member, IEEE, "*FPGA-Based 40.9-Gbits/s Masked AES With Area Optimization for Storage Area Network"*., 2013.
[2] Z. Yuan, Y. Wang, J. Li, R. Li, and W. Zhao, "FPGA based optimization for masked AES implementation," in *Proc. IEEE 54th Int. MWSCAS*, Seoul, Korea, 2011, pp. 1–4.
[3] National Institute of Standards and Technology, "Advanced Encryption Standard(AES)," FIPS-197, 2001.
[4] E. Prouff, M. Rivain and R. Bevan, "Statistical analysis of second order differential power analysis," IEEE Transactions on Computers, vol. 58, 2009, pp. 799-811.
[5] S. Mangard, E. Oswald and T. Popp. "Power analysis attacks: revealing the secrets of smart cards," Spinger-Verlag, 2007
[6] J. D. Golic, "Techniques for random masking in hardware," IEEE Transactions on Circuits and Systems, vol. 54, Feb. 2007, Pages: 291- 300.
[7] J. Wolkerstorfer, E. Oswald and M. Lamberger, "An ASIC implementation of the AES Sboxes," in CT-RSA 2002, vol. 2271, Springer-Verlag, 2002, pp. 67-78.
[8] Introduction to Storage Area Networks and System Networking by Jon Tate, Pall Beck, Hector Hugo Ibarra, Shanmuganathan Kumaravel and Libor Miklas.
[9] L. Ali, I. Aris, F. S. Hossain and N. Roy, "Design of an ultra-high speed AES processor for next generation IT security," Computers and Electrical Engineering, Vol.37 (6), pp.1160-1170, Nov. 2011.
[10] K.H. Chang, Y.C. Chen, C. C. Hsieh, C. W. Huang and C. J. Chang, "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application," IEEE International Symposium on Circuits and Systems, pp. 1922-1925, May 2009.
[11] J. M. G. Criado, M. A. V. Rodriguez, J. M. S. Perez, J. A. G. Pulido, "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration," Integration, the VLSI Journal, Vol.43(1), pp. 72-80, Jan. 2010.
[12] J. V. Dyken, J. G. Delgado-Frias, "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm," Journal of Systems Architecture, Vol.56(2–3), pp. 116-123, Mar. 2010.
[13] I. Hammad, K. E. Sankary and E. E. Masry, "High-Speed AES Encryptor With Efficient Merging Techniques," IEEE Embedded Systems Letters, Vol.2 (3), pp.67- 71, Sept. 2010.
[14] N. Ahmad, R. Hasan, W. M. Jubadi, "Design of AES S-Box using combinational logic optimization," IEEE Symposium on Industrial Electronics & Applications, pp.696-699, Oct. 2010.
[15] N. Ahmad, S. M. R. Hasan, "Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using Novel XOR Gate," Integration, the VLSI Journal, Article in Press.

ISSN: 2278 – 7798