Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 32-37, DOI: 10.14429/dsj.62.1439

Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box

Shristi Deva Sinha and Chaman Prakash Arya

Institute for Systems Studies and Analyses, Delhi – 110 054, India
E-mail: shristideva_issa@yahoo.com

ABSTRACT

Rijndael algorithm was selected as the advanced encryption standard in 2001 after five year long security evaluation; it is well proven in terms of its strength and efficiency. The substitution box is the back bone of the cipher and its strength lies in the simplicity of its algebraic construction. The present paper is a study of the construction of Rijndael Substitution box and the effect of varying the design components on its cryptographic properties.

Keywords: Advanced encryption standard, Rijndael, Rijndael algorithm, substitution box, cryptographic properties

1. INTRODUCTION

The advanced encryption standard (AES)* developed by Joan Daemen and Vincent Rijmen, Rijndael[1,2] was selected by National Institute of Standards and Technology (NIST) as in 2001. It is a symmetric block cipher-based on the Shannon substitution-permutation network. AES has long been an area of interest for the researchers due to its:

- Well proven security: A a 5-year evaluation procedure by NIST and it is designed to be resistant to linear, differential and mount attacks.
- Efficiency: The speed of encryption and decryption of AES is the fastest compared to any other cipher of similar strength.
- Design simplicity: The cipher has a simple and elegant structure that can easily be split into its components.

Most of the earlier works relating to AES are linked to its performance evaluation and straight forward implementation[3-7] including the various pipelined architecture. Some simplification[8,9] in the AES algorithm had been attempted. However, this simplifications lead to vulnerabilities[10] in the algorithm. A great amount of work has also been done in fast pipelined implementation[11-15] of the algorithm. Rijmen proposal of AES S-box implementation based on the composite fields[16] was a significant step to compact AES. Some work in optimum construction[17] of these composite fields has been done. Some study on the replacement[18] of the design parameters of the Rijndael algorithm has been done. It was suggested that this leads to creation of new ciphers equivalent in strength to the original. However, certain properties[19] of substitution box (S-box) has been identified, which are profoundly affected by the changes in design components. Recent works relating to AES S-box include the optimised implementation of the S-box using residues of prime numbers[20], a lightweight mix columns implementation for AES[21] and a proposal of a new algorithm to construct secure keys for AES[22] is published.

This paper focuses on the study of the algebraic construction of the S-box of the AES algorithm, which is the main strength of the cipher. The effect of the change in the design components of the S-box on its cryptographic properties has been analysed. It provides an insight to the AES S-box construction to generate a conceptual framework for all future customization of the algorithm targeted at the S-box design level.

2. BASIC STRUCTURE OF ADVANCED ENCRYPTION STANDARD

Full description of the AES algorithm can be obtained in FIPS[2] 197. The input and the output for AES are each bit sequences containing 128-bits. However, AES allows cipher keys of all 128-bits, 192-bits, or 256-bits lengths. The input 128 bits are arranged in a 4×4 matrix, termed the 'state' and all byte operations are performed in the Galois field GF(2^8). The cipher is specified in terms of repetitions of processing steps that are applied to make up rounds of keyed transformations between the input plain-text and the final output cipher-text. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key. The encryption of data is done in number of rounds:

a. Initial round: AddRoundKey
b. Rounds: SubBytes, ShiftRows, MixColumns, and AddRoundKey
c. Final round: SubBytes, ShiftRows, and AddRoundKey.

Addroundkey : Addroundkey is a XOR of the key with the array.
ShiftRows : ShiftRows cyclicly shifts the elements of the

Note: The terms Rijndael and AES have been used invariably throughout the paper as the input size is not of relevance in this particular study.
Received 23 November 2011, online published 23 January 2012

i^{th} row of the state C_i elements to the right, where, C_i are fixed constants C_i = 0, 1, 2 and 3.

MixColumns : The columns of the state are considered as polynomials over GF(2^8) and multiplied modulo x^4+1 by $03.x^3+x^2+02$ to give a new column array.

SubBytes : SubBytes is a nonlinear byte substitution, operating on each of the state bytes independently.

In all these operations, the SubBytes deserve a special mention as this step involves the S-box. The S-box is the back bone of the cipher; it provides nonlinearity in the encryption process and plays an important role in key scheduling.

3. ALGEBRAIC PRELIMINARIES AND S-BOX CONSTRUCTION

For the study of algebraic construction of the S-box a theorem is stated here without proof.

Theorem 1

Let *p* be a non-zero element of a principle ideal domain *R* then, *R*/(*p*) will be a field if and only if, *p* is irreducible[23].

According to this theorem, for a prime *p* Galios field $GF(p^n)$ is constructed by using a generating polynomial *m*(*x*) of degree *n* taking

$$GF(p^n) = \frac{GF(p)[x]}{m(x)}$$

In the AES algorithm, the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ is used to generate the underlying field $GF(2^8)$. All bytes *b* in Rijndael are interpreted as elements of this field represented by a polynomial $a_1 + a_2x + a_3x^2 + a_4x^3 + a_5x^4 + a_6x^5 + a_7x^6 + a_8x^7$ where, each bit $a_i \in GF(2)$ and $b \in GF(2^8)$. In this field, addition $\oplus$ and multiplication $\odot$ are defined by the XOR operation and polynomial multiplication modulo the generating polynomial respectively.

An S-box is a transformation $\sigma : GF(p^n) \rightarrow GF(p^n)$, In AES the S-box $\sigma : GF(2^8) \rightarrow GF(2^8)$ is constructed by substituting each element with its inverse and applying a suitable affine transformation $\sigma : X \rightarrow AX^{-1} + b$ where, $A \in GL_8(2)$, the general linear group of degree 8 over *GF*(2) and $b \in GF(2^8)$. Both of these *A* and *b* are fixed in AES:

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \text{ and } b = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

The motivation for this S-box design is to be resistant to differential, linear cryptanalysis and interpolation attacks. The core design is a simple transformation $x \rightarrow x^{-1}$ in *GF*(2^8), this mapping has a simple algebraic expression. However, the simplicity itself makes it vulnerable to attacks like the interpolation attack. Therefore, it is combined with a suitable affine transformation: $x \rightarrow Ax^{-1} + b$. The affine mapping is so chosen that, it has a very simple description, but a complicated algebraic expression. If combined with the 'inverse' mapping, it can be seen as modular polynomial multiplication followed by addition[1] $b(x) = (x^7 + x^6 + x^2 + x) + a(x)$ $(x^7 + x^6 + x^5 + x^4 + 1) \bmod (x^8 + 1)$. The purpose of the constant translation vector *b* is to ensure that $\exists$ no fixed and conjugate fixed points (i.e. $\exists$ no $x \in GF(2^8)$ such that $\sigma(x) = x$ or $\sigma(x) = \bar{x}$) in the S-box.

4. CHARACTERISTICS OF A GOOD S-BOX AND BIAS PARAMETERS

To study the characteristics of a good S-box $\sigma : GF(p^n) \rightarrow GF(p^n)$, it is realised as vectorial Boolean function $\sigma(x) = (\sigma_1(x), \sigma_2(x), ..., \sigma_n(x))$ where, each σ_i is a Boolean function of the Boolean variables $x_1, x_2 ....., x_n$.

Characteristics of the good S-box are, it has to:

- be balanced
- satisfy propagation criterion
- satisfy correlation immunity criterion
- have input/output bit-to-bit entropy (*H*) = 1.
- its nonlinearity (*N*) has to be = 120.
-

Each of these criteria's are explained in the following subsection. However, most of these are satisfied only for an ideal case and not in practical level. So, biases from each of these criterions are derived.

4.1 Balancedness Property

This property states that each of the Boolean functions of the S-box should be balanced, i.e., the number of ones and zeros in the truth table of the Boolean function must be equal.

4.2 Propagation Criterion

A Boolean function is said to satisfy propagation criterion of degree *k* and order *m*, if any function obtained by keeping *m* input bits fixed *f*(*x*) changes with probability half, whenever *i* ($1 \leq i \leq k$) bits of *x* are complemented.

Mathematically, by fixing *m* number of bits ${}^nC_m 2^m$ set of functions *g* are obtained from *f*, let it be denoted by *F*. Let $\alpha \in GF(2^n) : W(\alpha) \in [1, k]$ then a function is said to satisfy the propagation criterion of degree *k* and order *m*, if for each $g \in F$, $g(x) \oplus g(x \oplus \alpha)$ is balanced.

The propagation criterion is the measure of randomness of the differences in output pairs to the input pairs. This is a very important criterion as the bias of the distribution of the differences of the output pairs and the input pairs is utilised in the differential cryptanalysis of the conventional ciphers.

Definition

Propagation criterion bias of a Boolean function of degree *k* and order *m* is defined by[19]:

$$PCB_{\sigma_i}(k,m) = \max_{\alpha \in A\ g \in F} \left| \sum_{x \in F_2^n} (g(x) \oplus g(x \oplus \alpha)) - 2^{n-m-k} \right|$$

where $A = \{\alpha \in GF(2^n) : w(\alpha) \in [1,k]\}$.

For the S-box: $PCB_{\sigma}(k,m) = \max_{\sigma_i} PCB_{\sigma_i}(k,m)$

The propagation criterion of degree one and order zero is very well known criterion, termed as the strict avalanche criterion (SAC). The criterion is satisfied, if whenever a single input bit is complemented, each of the output bits changes with a probability $\frac{1}{2}$.

4.3 Correlation Immunity Criterion

A Boolean function is to satisfy a correlation immune of order *m*, if it is statistically independent of combination of any *m* input bits. Mathematically, if *m* input bits are fixed then the functions *g* obtained from Boolean function *f* must satisfy:

$$W(g) = \frac{W(f)}{2^m}$$

where *W*(*f*) denotes the Hamming weight of a Boolean function given by the number of *x* for which the function attains a non-zero value.

Definition : The correlation immunity bias of order *m* for a Boolean function is defined by[19]:

$$CIB_f(m) = \max_{f \in A} \left| 2^m \times W(g) - W(f) \right|$$

The correlation immunity bias of S-box is given by

$$CIB_{\sigma}(m) = \max_{i \in [1,s]} CIB_{\sigma_i}(m)$$

4.4 Input/output Bit-to-Bit Entropy

This parameter represents the amount of information about the value of input bit, if the value of the output bit is known. The entropy of a single output function is given by[24]:

$$H(P_i) = P_i \log_2(\frac{1}{P_i}) + (1 - P_i) \log_2(1 - P_i)$$

where P_i, is the fraction of 1's in the output column of the truth table.

Definition : The $(i,j)^{th}$ Input/output bit-to-bit entropy $H(x_i / \sigma_i(x))$ is computed and the parameter is defined[19] by $H = \min_{i,j \in [1,n]} H(x_i / \sigma_j(x))$.

4.5 Nonlinearity

An affine Boolean function does not provide an effective confusion. To overcome this, functions which are as far as possible from being an affine function are needed. The effectiveness of these functions is measured by a parameter called nonlinearity.

Definition : Nonlinearity of a Boolean function is measured by the Hamming distance to the set of affine functions[25]

$$N(f) = 2^{n-1} - \frac{1}{2} \times \max_{w \in F_2^n} F(w)$$

where *F* is the Walsh transformation of *f*,

$$\text{For S-box } N = \min_{i \in [1,n]} (N(f_i))$$

For good cryptographic properties of the S-box, these parameters should have the values[19]: H = 1, PCB(1,0) = 0, PCB(1,1) = 0, CIB(1) = 0 and nonlinearity, *N* = 120. However, values of these parameters for the AES S-box are: H = 0.9887, PCB(1,0) = 16, PCB(1,1) = 20, CIB(1) = 16 and nonlinearity *N* = 112. The values of these bias parameters are used to analyze the effect of changes in the design components of the AES S-box on its cryptographic properties. Different possible variations on the S-box components and their affects have been discussed in the next section.

5. ANALYSIS AND RESULTS

The S-box is constructed by the transformation:

$x = Ax^{-1} + b$, where, $x \in GF(2^8)$,

$A \in \text{GL}_8(2)$ and $b \in GF(2^8)$.

All the variations in its construction without altering the simple algebraic expression are looked into and their effects in the bias parameter values are analysed. One of the major changes that can be brought about without altering the algebraic expression is by changing the underlying field to isomorphic fields. Another option is to change the affine matrix *A* and third is changing the vector *b*.

5.1 Change in the Underlying Field to Isomorphic Fields

Isomorphic fields to the underlying field can be generated by using different irreducible polynomials of the same degree. Number of irreducible polynomials of degree *n* over GF(*p*) is given by:

$\frac{1}{n}\sum_{d/n} \mu(d) p^{n/d}$, where μ *is* the Mobius function.

$$\mu(n) \equiv \begin{cases} 0 & \text{if } n \text{ has 1 or more repeated prime factors} \\ 1 & \text{if } n=1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \end{cases}$$

Thus, ∃ a total of 30 irreducible polynomials of degree 8 over GF(2) including the one originally used. The irreducible polynomials are constructed by generating the polynomials and testing their irreducibility using the following theorem:

Theorem 2: Rabin's Test for irreducibility[26]

A polynomial $C \in GF(p)[x]$ of degree *d* is irreducible if and only if $X^{p^d} = x \bmod C$

The irreducible polynomials and the values of the bias parameters of the respective S-boxes constructed on isomorphic field generated by them are shown in Table 1.

It can be observed from Table 1 that values of the bias parameters can be enhanced on changing to isomorphic fields as in the case of the irreducible polynomial $x^8 + x^6 + x^5 + x + 1$.

Table 1. Generating polynomials and the corresponding parameter values of the S-boxes

Generating Polynomials	H	PCB (1,0)	PCB (1,1)	CIB(1)
$x^8+x^4+x^3+x+1$ (AES)	0.9887	16	20	16
$x^8+x^7+x^5+x^4+1$	0.9914	16	20	14
$x^8+x^6+x^5+x^4+1$	0.9914	16	20	16
$x^8+x^4+x^3+x^2+1$	0.9914	16	20	16
$x^8+x^7+x^6+x^4+x^3+x^2+1$	0.9887	16	20	16
$x^8+x^6+x^5+x^4+x^2+x+1$	0.9914	16	18	14
$x^8+x^5+x^3+x+1$	0.9914	16	20	16
$x^8+x^7+x^5+x^3+1$	0.9914	16	20	14
$x^8+x^7+x^6+x^5+x^4+x^3+1$	0.9887	16	20	16
$x^8+x^5+x^4+x^3+x^2+x+1$	0.9914	16	20	14
$x^8+x^7+x^6+x^4+x^2+x+1$	0.9914	16	20	16
$x^8+x^5+x^3+x^2+1$	0.9937	16	20	16
$x^8+x^6+x^5+x^3+1$	0.9914	16	20	16
$x^8+x^7+x^4+x^3+x^2+x+1$	0.9914	12	20	16
$x^8+x^7+x^6+x^5+x^4+x+1$	0.9887	16	20	14
$x^8+x^5+x^4+x^3+1$	0.9937	12	18	16
$x^8+x^7+x^5+x+1$	0.9914	16	18	14
$x^8+x^7+x^3+x+1$	0.9887	16	20	16
$x^8+x^6+x^5+x^2+1$	0.9937	16	20	12
$x^8+x^6+x^3+x^2+1$	0.9887	16	20	16
$x^8+x^7+x^5+x^4+x^3+x^2+1$	0.9887	16	20	16
$x^8+x^6+x^5+x^4+x^3+x+1$	0.9887	12	20	16
$x^8+x^6+x^4+x^3+x^2+x+1$	0.9914	16	20	16
$x^8+x^7+x^6+x^5+x^4+x^2+1$	0.9937	16	20	14
$x^8+x^7+x^3+x^2+1$	0.9914	16	24	14
$x^8+x^6+x^5+x+1$	0.9914	12	18	14
$x^8+x^7+x^6+x^5+x^2+x+1$	0.9887	16	20	16
$x^8+x^7+x^6+x^3+x^2+x+1$	0.9914	16	20	16
$x^8+x^7+x^2+x+1$	0.9887	12	20	16
$x^8+x^7+x^6+x+1$	0.9914	16	20	14

5.2 Change in the Affine Matrix

Another variation in the S-box design component can be brought about by changing the affine matrix A. The affine matrix $A \in GL_8(2)$, the general linear group of degree 8 over GF(2) and the order of this group is:

$\prod_{k=0}^{7}(2^8-2^k) \sim 5.3481 \times 10^{18}$.

Hence, the number of matrix A available to be used for varying the S-box is numerous. So, to analyse the effect of such change on the bias parameter values instead of performing an exhaustive search over this group, a random search has been done. For this, a square binary matrix of size 8 is randomly generated. The matrix is discarded, if found to be singular and another matrix is generated again. This non-singular randomly generated matrix is used in the construction of S-box and the bias parameters are computed. This process is implemented in MatLab and is repeated 500 times. Few randomly generated affine matrices obtained on 500 such random searches are:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and $$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Some of the observed bias parameter values obtained due to the change in the affine matrix in the random search are shown in Table 2.

Table 2. Values of the bias parameters obtained for different affine matrix

H	PCB(1,0)	PCB(1,1)	CIB(1)
0.989	16	20	14
0.991	16	20	8
0.991	14	20	12

5.3 Change in the Translation Vector

The translation vector $b \in GF(2^8)$ and $O(GF(2^8)) = 256$ therefore, $\exists$ total 256 different vector b (including the one used in the AES) that can be used in the S-box construction. However, it is observed that change in the translation vectors has no impact on the values of the bias parameters. Only the number of fixed and conjugate fixed points of the S-box varies with it. It was observed that the nonlinearity (N=112) of the AES S-box was not affected by any of the above mentioned changes.

6. CONCLUSIONS

Rijndael algorithm accepted as the AES is a well proven and an efficient cipher. The S-box forms a backbone of this cipher and is designed with a very simple algebraic expression. This paper studies the construction of its S-box and explores the possible design variations without altering its simple algebraic expression. The effect of these changes on the cryptographic properties of the S-box has also been analysed. The main aim of this study is to provide an insight to the AES S-box construction to generate a conceptual framework for all possible customization on the cipher targeted at the S-box design level. It is observed that by changing the underlying field into the isomorphic fields improves the properties to some level. A similar effect is observed for the change in the affine matrix. However, change in the translation vector shows no effect in the cryptographic properties of the S-box.

ACKNOWLEDGEMENTS

The authors would like to thank Shri H.V. Srinivasa Rao Director, Institute for Systems Studies and Analyses, DRDO for his encouragement and support in this work. The authors would also like to thank Shri P.K. Bhatnagar and Shri Yogesh Chandra for their kind suggestions and guidance.

REFERENCES

1. Daemen, J. & Rijmen, V. AES Proposal: Rijndael (Version 2), 1999. http://csrc.nist.gov/publications/ [Accessed on 9 June 2009].
2. National Institute of Standards and Technology, Advanced encryption standard (AES). (FIPS 197), 2001. http://csrc.nist.gov/.publications/ [Accessed on 11 June 2009].
3. Dandalis, A.; Prasanna, V.K. & Rolim, J.D. A comparative study of performance of AES final candidates using FPGAs. Cryptographic Hardware and Embedded Systems Workshop, Worcester, Massachusetts, 2000, 125-40.
4. Elbirt A. J.; Yip, W.; Chetwynd, B. & Paar, C. An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists. *IEEE Trans. Very Large Scale Integration Syst.*, 2000, **9**(4), 545-57.
5. Gaj, K. & Chodowiec, P. Hardware performance of the AES finalists-survey and analysis results. 2000, http://ece.gmu.edu/crypto/AES_survey.pdf [Accessed on 28 June 2009].
6. Ichikawa, T. & Matsui, T. Hardware evaluation of the AES finalists. In the 3rd Advanced Encryption Standard Candidate Conference, New York, 2000, 279-85.
7. Mali, M.; Novak, F. & Anton, B. Hardware implementation of AES algorithm. *J. Electrical Engg.*, 2005, **56**(9-10), 265-69.
8. Feldhofer, M.; Wolkerstorfer, J. & Rijmen, V. AES implementation on a grain of sand. *IEE Proc. Infor. Security*, 2005, **152**(1), 13-20.
9. Canright, D. A very compact Rijndael S-box. Naval Postgraduate School, Monterey, California, Report no. NPS-MA-04-001, May 2005.
10. Mansoori, S.D. & Bizaki, H.K. On the vulnerability of simplified AES algorithm against linear cryptanalysis. Inter. *J. Comp. Sci. Network Security*, 2007, **7**(7), 257-63.
11. Fischer, V. & Drutarovsky, M. Two methods of Rijndael implementation in reconfigurable hardware, cryptographic hardware and embedded systems. *In* Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems, Paris, 2001, 77-92.
12. McLoone, M. & McCanny, J.V. High performance single-chip FPGA Rijndael algorithm implementations. *In* Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems, London, 2001, 65-76.
13. McLoone, M. & McCanny, J.V. Single-chip FPGA implementation of the advanced encryption standard algorithm, field-programmable logic and applications. *In* Proceedings of the 11th International Conference on Field-Programmable Logic and Applications, UK, 2001, 152-61.

14. McLoone, W. & McCanny, J.V. Rijndael FPGA implementation utilizing look-up tables. *In* IEEE Workshop on Signal Processing Systems, Belgium, 2001, 349- 60.
15. Chodowiec, P.; Gaj, K. & Mason, G. Very compact FPGA implementation of the AES algorithm. *In* the 5th International Workshop on Cryptographic Hardware and Embedded Systems. USA, 2003, 319-33.
16. Rijmen, V. Efficient implementation of the Rijndael S-box, Belgium, http://www.esat.kuleuven.ac.be/~rijmen/rijndael/sbox.pdf [Accessed on 28 June 2009].
17. Zhang, X. & Parhi, K.K. On the optimum constructions of composite field for the AES algorithm. *IEEE Trans. Circuits and Systems-II*, 2006, **53**(10), 1153-57.
18. Barkan, E. & Biham, E. In how many ways can you write Rijndael? *In* Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 2002, 160-75.
19. Otokar, G.; Spyros, M.; Jan, T. & Wandi, W. Is Rijndael really independent of the field polynomial? *Tatra Mt. Publ*., **33**, 2006, 51-69.
20. Abuelyman, E.S. & Alsehibani, A.S. An optimized implementation of the S-Box using residues of prime numbers. Inter. *J. Comp. Sci. Network Security*, 2008, **8**(4), 304-09.
21. Ahmed, E.G.; Shaaban, E. & Hashem, M. Lightweight mix columns implementation for AES. *In* Proceedings of the 9th International Conference on Applied Informatics and Communications, Wisconsin, USA, 2009, 253-58.
22. Mahmood, H. A new algorithm to construct secure keys for AES. *Int. J. Contemporary Mathematical Sci.*, 2010, **5** (26), 1263-270.
23. Artin, M. Algebra. Prentice Hall, USA 1991. 618 p.
24. Cheng, K. & Agrawal, V.D. An entropy measure for the complexity of multi-output boolean functions. *In* Proceedings of the 27th ACM/IEEE Design Automation conference, 1991, 302-05.
25. Rothaus, O.S. On bent functions. *J. Combinatorial Theory (A)*, 1976, **20**, 300-05.
26. Jörg, A. Testing polynomial irreducibility without GCDs. Institut National De Recherche En Informatique Et En Automatique (INRIA), France, Report No. 6542, May 2008.

Contributors

Mr Shristi Deva Sinha received his MSc (Mathematics) from University of North Bengal, Darjeeling. Currently, he is working as a Scientist in the Institute for Systems Studies & Analyses (ISSA), DRDO, Delhi. He has been involved in the analysis of naval weapon systems/ procedures and cryptography.

Mr Chaman Prakash Arya received his MSc(Mathematics) from University of Delhi, Delhi. He is presently pursuing PhD in General Topology from University of Delhi. Currently, he is working as a Scientist in the ISSA, DRDO, Delhi. He has been involved in the area of OLI evaluation of weapons and cryptography.