International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

A Novel S-box Generation of AES using Elliptic Curve Cryptography (ECC)

Sapna Kumari. C, K. V. Prasad

Abstract: ***In recent decades, the security of the data is playing a major role in communication systems due to more attackers between the channel media. The security level is depending on secret key, as per literature survey of ECC guide, higher the bits size of the keys, higher the security [19]. Therefore the generation of key with large size is the major challenging task. At present, Advanced Encryption Standard (AES) is a better cryptography system where the encryption and decryption can be performed with fixed key size of 128bits, 192 bits and 256 bits. The security level has been increased in AES due to the S-Box and it consists of 256 different values in the form of 16x16 matrixes, but to generate 256 values the Galois Field (GF) has been used. GF requires a lot of hardware resources with more number of arithmetic operations like multiplication, additions and inversions [20-21]. To overcome this issue, a novel S-Box generation using Elliptic Curve Cryptography (ECC)and BWMC methods are proposed. The ECC uses point addition and point doubling to generate 256 values without multiplication operations. After generation of the matrix, its values are encrypted and decrypted using bitwise matrix code (BWMC). The proposed work has been designed using Verilog HDL, simulated and validated on Vertex-5 FPGA development board. From the results obtained from novel S-Box and BWMC techniques there is an improvement in terms of delay i.e. 73.1% as compared with hamming codes and 69% improvement in speed as compared with MC's[22].***

Index Terms: AES, BWMC, ECC, Point addition, point doubling, FPGA, Security system and S-Box.

I. INTRODUCTION

With the evolution of the technology in recent times, the research scholars and industries are trying to find some solution to avoid the hacking information between the sender and the receiver. To make the data transfer secure through communication media, ECC cryptography is best solution and it is secure compared to all other cryptography methods like BCH, RC1 to RC 6, RS codes and hamming codes. ECC generates different size of keys and also deals with the encryption and decryption of the given data. It uses both private and public key cryptography. The public key cryptography system provides more security, hence ECC is one such cryptographic method[23] where one could rely on it for security purpose . The main advantage of ECC over RSA is that ECC has supported smaller to larger key sizes depending upon the applications and requirements, thereby the processing complexity will be reduced [1].

Manuscript published on 28 February 2019.
*Correspondence Author(s)
Sapna Kumari C, Ph.D Research Scholar, Jain University, Bangalore
K.V.Prasad, Professor & HOD, Department of ECE, Bangalore Institute of Technology, Bangalore

The point addition, point doubling and scalar multiplications are main operations of ECC to find points on the curve. These point operations are helping us to perform the encryption and decryption operations. The Elgamal method is one such point generation operation and it is a part of ECC operation. It also supports static i.e., one to one mapping methods and dynamic (one to N mapping methods) explained in [2]. Static is a simple technique, the same alphanumeric characters from the different words are always mapped onto the same x-y coordinates of the elliptic curve points. When encrypted, points obtained will also be the same. Therefore, an intruder can easily interpret the data with trial and error methods hence the secrecy of data transmission by using this methodology is very low. In dynamic mapping, the alphanumeric characters are mapped dynamically on to the points of EC. The issues of cryptography system to exchange the information between the sender/transmitter and the receiver/user can be minimized using ECC. Diffie- Hellmen-Merkle key, exchange by performing scalar multiplication to generate the points likeP,2P,3P,4P,…….563P (As per ECC guide, higher the key size, better the security and p must be a any prime number). The generated point P=f(x,y), is used to obtain 563 points . Point addition and point doubling methods will avoid complex arithmetic operation like multiplication and divisions thereby the complexity of the system is reduced and thus its speed can be improved[22]

The sender encrypts the message using Elgamal methodfor different key sizes and decrypts the original message using same key sizes [3,12]. Reed Solomon codes to speed up the process with transmission speed of 200Mbits/sec[15]. The transmitter computes the message into $(M + M_s * (M_R * G))$, where M is message, M_s is sender message, $M_R$is receiver message and G is generator point and the message which is encrypted by $(M_s * G, M + M_S * (M_R * G))$ and memories error corrections presented in [4]. The sender key computes $K_R * (M_s * G)$ and receiver decrypts the data by using $M + M_s * (M_R * G) - K_R * (M_s * G)$ in [5-6]. It has a high reliability and can reduce redundant bits in memory devices. The NoC and SoC devices require high speed and reduced redundant operations, thus these designs are linear and the block codes are presented in [7-8]. The multiple bit error correction, soft error tolerance devices like Content Addressable Memories (CAMs) and soft error corrections for memories like SRAM and others memory devices have been proposed in [9-10, 13-14].The data transfer switching devices like NoC and SoC systems require the error correction techniques to decode the data at receiver and effective control of data transfer is presented in [16-18].

II. METHODOLOGY

The advanced encryption standard (AES), encrypted and decrypted bits are of size 128 bits, 192 bits and 256bits for 8,10,12 round operations. The cipher text is 128 bits and it is denoted as Nk-8, the Byte substitution, shift rows, add round key and Mixcolumns process is based on 4 Byte substitutionsand are divided into 4x4 arrays consisting of 16 bytes.Each byte value is replaced by corresponding S-Box values,which is generated by ECC. S-Box is encrypted and decrypted using BWMC for more security.Thesubstitution box can be created using just two arithmetic operations such as addition and doubling to reduce the FPGA hardware resources and for faster operations of encryption and decryption. To use ECC, the following conditions should be satisfied and in elliptic curve cryptography the ECC curve is restricted from defining the curve in finite field (F_p). The interesting concept of cryptograph is defining over the elliptic curves group with modulo operation mod p and p is defined in ECC is any large prime numberdefined as given in eq. (1).

$$4a_1^3+27b_1^2 \pmod p \neq 0 \qquad \text{---- (1)}$$

Here the a_1 and b are two are nonnegative integer numbers, considered $a_1=1$, $b_1=1$ and p=563.Then $E_p(a_1, b_1)$ indicates the elliptic curve group mod p whose elements (x, y) are twosomes of nonnegative integers less than p, as given in eq. (2)

$$y^2=[x^3+ a_1x+ b_1] \pmod p \qquad \text{----- (2)}$$

The equation (2) is separated into LHS and RHS to find the initial point on the elliptic curve.

$$\text{LHS}= y^2 \bmod p \qquad \text{----- (3)}$$

$$\text{RHS}=[x^3+ a_1x+ b_1] \pmod p= [x^3+x+1] \pmod p \text{----- (4)}$$

The calculated values of LHS are listed in Table-I and RHS values are listed in Table-II.

ECC point operations

In point addition, given 2 arguments on an elliptic curve, J(x_1, y_1) and K(x_2, y_2), then the addition of these points results in L(x_3, y_3) which lies on the curve as shown in Fig.1.

$$\lambda = [(y_2-y_1)/(x_2-x_1)] \pmod p$$

$$x_3= [\lambda-x_1-x_2] \pmod p$$

$$y_3= [\lambda(x_1-x_3)-y_2] \pmod p$$

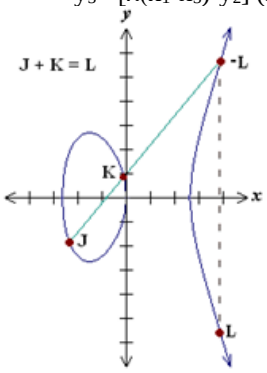


Fig 1. Point addition operation on ECC

In point doubling, given a point J(x_1, y_1) on an elliptic curve, point doubling i.e. J(x_1, y_1) + J(x_1, y_1) yields L(x_3, y_3) which lies on that curve as shown in Fig.2.

$$\lambda = [(3x_1^2 + a_1) / (2y_1)] \pmod p$$

$$x_3=[\lambda-2x_1] \pmod p$$

$$y_3= [\lambda(x_1-x_3)-y_2] \pmod p$$

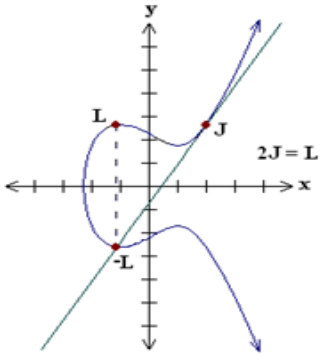


Fig.2. Point doubling operation on elliptic curve

In point negative, given a point J(x_1, y_1) on an elliptic curve, to find -J(x_1, y_1) is given by J(x_1, p- y_1), as shown in Fig 3.

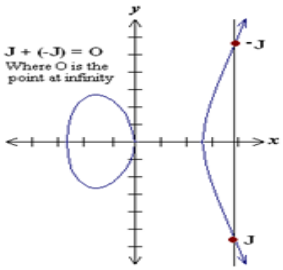


Fig.3. Point Negative operation on elliptic curve

Scalar Multiplication

Given a point P(x_1, y_1) on an elliptic curve, to compute Q(x_2,y_2) = k P(x_1, y_1), where k is any integer, it needs repeated point addition and point doubling. The computed point are stored in ROM memoryto perform write and read operation. The size of each memory location is 32bits and total number of memory locations are 256. All the 256 points are in form of 16x16 matrix and each point size is 32bits. The input data is replaced with S-box values based on x and y coordinate values as shown in BWMC.Suppose the input data is 4512, the first digit is x-coordinate i.e 4 and the last digit is y-coordinate i.e 2. The value 4512 is replaced by fourth column and second row values from S-box. The result of S-box value.is encrypted using BWMC and an encrypted data is transmitted through wireless communication. The received data at receiver is decrypted using syndrome calculator and error detector circuit. The table III shows the points on elliptic curve.The S-box value is mapped on to the points on an elliptic curve. Based on the input values, the S-Box values are replaced for next encryption and decryption using BWMC.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 1:S-box value

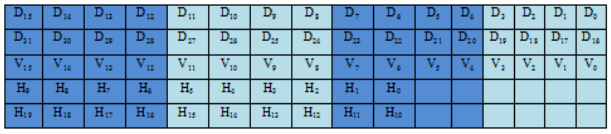
Points	Points on the elliptic curve				
1-5	(70,86)	(270,328)	(226,429)	(104,86)	(294,324)
6-10	(73,287)	(179,19)	(390,302)	(182,394)	(299,334)
11-15	(82,271)	(304,401)	(223,82)	(292,148)	(268,134)
16-20	(373,216)	(8,153)	(321,232)	(283,100)	(256,280)
21-25	(258,161)	(122,327)	(68,226)	(235,354)	(102,36)
26-30	(132,197)	(392,383)	(244,241)	(95,384)	(137,59)
31-35	(438,394)	(34,294)	(78,166)	(139,377)	(137,336)
36-40	(449,340)	(8,410)	(90,109)	(324,409)	(14,150)
41-45	(437,135)	(334,59)	(237,10)	(263,414)	(246,289)
46-50	(430,454)	(374,200)	(8,273)	(228,286)	(253,407)
51-55	(296,269)	(428,80)	(236,222)	(339,6)	(217,315)
56-60	(304,391)	(157,412)	(432,204)	(251,274)	(15,11)
61-65	(24,103)	(442,132)	(112,327)	(126,378)	(306,337)
66-70	(73,53)	(441,291)	(355,406)	(87,33)	(178,115)
71-75	(110,452)	(16,84)	(424,261)	(253,73)	(162,144)
76-80	(328,293)	(247,165)	(276,402)	(13,93)	(452,275)
81-85	(358,123)	(166,56)	(417,225)	(117,365)	(175,197)
86-90	(225,44)	(433,96)	(29,279)	(157,380)	(330,137)
91-95	(206,158)	(29,451)	(10,80)	(258,173)	(139,52)
96-100	(126,102)	(97,237)	(67,144)	(53,64)	(284,209)
101-105	(203,108)	(83,347)	(272,346)	(13,267)	(366,131)
106-110	(328,258)	(14,260)	(162,51)	(187,34)	(374,154)
111-115	(14,24)	(69,97)	(445,335)	(186,367)	(56,371)
116-120	(64,321)	(384,20)	(443,363)	(237,409)	(409,185)
121-125	(328,147)	(214,121)	(31,454)	(27,458)	(75,108)
126-130	(82,56)	(433,127)	(239,162)	(376,12)	(82,14)
131-135	(347,187)	(306,195)	(205,348)	(321,298)	(73,380)
136-140	(59,348)	(423,72)	(299,162)	(407,158)	(125,376)
141-145	(93,382)	(437,4)	(182,127)	(399,134)	(315,292)
146-150	(93,369)	(370,128)	(241,66)	(209,266)	(188,434)
151-155	(308,452)	(146,289)	(428,164)	(318,58)	(330,257)
156-160	(69,351)	(173,355)	(282,395)	(58,80)	(451,418)
161-165	(11,172)	(81,189)	128,339)	(132,441)	(384,222)
166-170	(212,225)	(230,155)	(37,17)	(104,348)	(162,440)
171-175	(155,60)	(217,199)	(357,443)	(167,166)	(415,160)
176-180	(419,280)	(282,356)	(175,78)	(31,83)	(36,304)
181-185	(4,19)	(234,274)	(295,232)	(441,334)	(303,142)
186-190	(444,412)	(204,332)	(62,136)	(399,234)	(150,333)
195-200	(329,104)	(172,205)	(286,18)	(44,334)	(303,142)
201-205	(444,412)	(204,332)	(62,136)	(399,234)	(107,275)
206-210	(51,424)	(152,221)	(52,222)	(91,223)	(19,224)
211-215	(101,227)	222,229)	(81,230)	(104,231)	(113,232)
216-220	(114,196)	(62,199)	(126,200)	(149,200)	(191,200)
221-225	(18,190)	(130,191)	(79,192)	(78,193)	(77,194)
226-230	(119,132)	(85,134)	(148,138)	(176,143)	(25,144)
231-235	(199,144)	(73,147)	(171,148)	(58,153)	(179,154)
236-240	(231,154)	(132,159)	(2,160)	(54,160)	(177,160)
241-245	(20,161)	(128,163)	(204,163)	(37,166)	(183,168)
246-250	(46,119)	(1,121)	(30,121)	(219,124)	(72,125)
251-255	(4,126)	(181,126)	(36,127)	(120,131)	(108,132)
256	(0,233)				

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

III. BWMC ENCRYPTION AND DECRYPTION

BWMC algorithm is adopted in the proposed BWMCencryption and Decryption methods to increase the security level, error detection and correction capability for the generated S-Box values. In this algorithm, power consumed is less compared to other detection methods [23]. BWMC involves bitwise integer subtraction and integer addition. In the bitwise algorithm,the data is dividedinto 4 bits andit is arranged in the form matrix tocarry out for further operations. The N-bit word is represented in the divided form, n symbols of m bits (N = n × m). These symbols are placed in a two-dimensional matrix of n= n1 × n2 (n1- number of columns, n2- number of rows). Through fractionnumber addition on cryptograms ineach row, the horizontal dismissed bits 'H' are obtained. Binary operation on the bits per column gives the vertical redundant bits 'V'. The symbols divided and arranged in matrix form are presented in logical format.

The information data is 32 bit in word (D_0 to D_{31}) and it is divided into 8 symbols and each symbol is 4 bits as shown below



symbol 0= D_0 to D_3
symbol 1= D_7 to D_4
symbol 2= D_{11} to D_8
symbol 3= D_{15} to D_{12}
symbol 4= D_{19} to D_{16}
symbol 5= D_{23} to D_{20}
symbol 6= D_{27} to D_{24}
symbol 7= D_{31} to D_{28}

Bits from H_0 to $H_{19}$are horizontal check bits and V_0 to V_{15} are vertical check bits. As shown in Equation (5) to (8) by decimal integer addition horizontal redundant bits 'H' are obtained,

$H_4\ H_3\ H_2\ H_1\ H_0 = D_3\ D_2\ D_1\ D_0 + D_{11}\ D_{10}\ D_9\ D_8$ ----------5

$H_9\ H_8\ H_7\ H_6\ H_5 = D_7\ D_6\ D_5\ D_4 + D_{15}\ D_{14}\ D_{13}\ D_{12}$ ----------6

$H_{14}\ H_{13}\ H_{12}H_{11}\ H_{10} = D_{19}\ D_{18}\ D_{17}\ D_{16} + D_{27}\ D_{26}\ D_{25}\ D_{24}$ ----------7

$H_{19}H_{18}\ H_{17}H_{16}\ H_{15} = D_{23}\ D_{22}\ D_{21}\ D_{20} + D_{31}\ D_{30}\ D_{29}\ D_{28}$ ----------8

Similarly remaining horizontal redundant bits are obtained. Here '+'represents bitwise integer addition. The vertical redundant bits 'V'can be obtained from XOR operation as given below in the equations :

$V_0 = D_0 \oplus D_{16}$
$V_1 = D_1 \oplus D_{17}$
$V_2 = D_2 \oplus D_{18}$
$V_3 = D_3 \oplus D_{19}$
$V_4 = D_4 \oplus D_{20}$
$V_5 = D_5 \oplus D_{21}$
$V_6 = D_6 \oplus D_{22}$
$V_7 = D_7 \oplus D_{23}$
$V_8 = D_8 \oplus D_{24}$
$V_9 = D_9 \oplus D_{25}$
$V_{10} = D_{10} \oplus D_{26}$
$V_{11} = D_{11} \oplus D_{27}$
$V_{12} = D_{12} \oplus D_{28}$
$V_{13} = D_{13} \oplus D_{29}$
$V_{14} = D_{14} \oplus D_{30}$
$V_{15} = D_{15} \oplus D_{31}$

The encoding is be done by decimal and binary addition operations. The encryptioncalculates the dismissed bits using XOR gates and multi bit adders. Where, H19−H0 are horizontal redundant bits.

V15−V0 are vertical dismissed bits.

U31−U0 are the information bits directly taken from D31 to D0

BWMC Decryption

Decoding process is needed to detect and correct errors in the word obtained from the encryption output. Let us suppose that the bits *B*3, *B*2, *B*1, and *B*0 are original information bits and the bits *C*0 and *C*1 are redundant bits. The bits *C*0 and *C*1 are obtained using the binary algorithm (XOR operation)

$C0 = B0\ \text{xor} B2 = 1\ \text{xor} 0 = 1$
$C1 = B1\ \text{xor} B3 = 0\ \text{xor} 1 = 1.$

Then assume now that MCUs occur in bits *B*3, *B*2, and *B*0, the received redundant bits *C*0 and *C*1 are computed

$$C_0' = B_0' xor B_2' = 0\ xor\ 1 = 1$$
$$C_1' = B_1' xor B_3' = 0\ xor\ 0 = 0$$

In order to detect these errors, the syndrome bits *S*0 and *S*1 are obtained

$$S_0 = C_0' xor C_0 = 1 xor\ 1 = 0$$
$$S_1 = C_1' xor C_1 = 0\ xor\ 1 = 1$$

These results mean that error bits *B*2 and *B*0 are wrongly regarded as the original bits so that these two error bits arenot corrected. This example illustrates that for this simple binary operation, the number of even bit errors cannot be detected. At the commencement, from the received information bits 'D' the received redundant bits $H_4\ H_3\ H_2\ H_1\ H_0$and $V_0^1 - V_3^1$ are generated. Using equation 9 and 10 the horizontal syndrome bits $H_4\ H_3\ H_2\ H_1\ H_0'$and the vertical syndrome bits S3 −S0 are calculated as follows:

$$\Delta H_4H_3H_2H_1H_0^1 = H_4H_3H_2H_1H_0^1 - H_4H_3H_2H_1H_0$$

----------9

$$S_3 - S_0 = V_0^1 \oplus V_0$$ ----------10

Similar calculations are done for the remaining vertical syndrome bits. Here"–" is the decimal integer subtraction. When $\Delta H_4H_3H_2H_1H_0^1$and $S_3 - S_0$are equal to zero, then the stored code word has only original information bits in the symbols and no errors. When $\Delta H_4H_3H_2H_1H_0^1$and $S_3 - S_0$are nonzero, then there is an error. Induced errors are detected in symbol 0. These errors are corrected by using equation 11.

$$D_{0correct} = D_0 \oplus S_0$$ ----------11

In a similar manner the errors in the other symbols viz, symbol 1, symbol 2 etc are detected and corrected.

IV. RESULTS AND DISCUSSION

The proposed work is designed and developed as a hardware prototype module for low power, low area and lesser delay using ECC. BWMC encryption and decryption by incorporating point addition and point doubling to generate 256 points to create S-Box.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The developed prototype module includes 256 points key generation, ROM memory creation, BWMC encryption and decryption to consume less number of hardware resources.

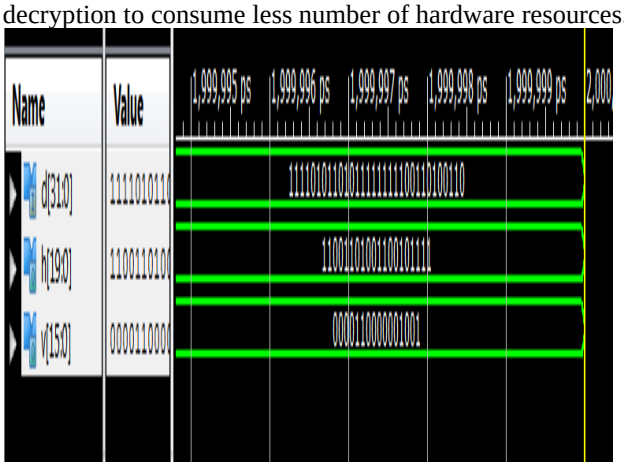


Fig.4. BWMC encryption output in Xilinx Isim simulator

The 32 bits data'd' in the Fig.4. is the point on the ECC curve that needs to be applied on BWMC for encryption, which uses integer addition between different symbols to get encrypted or cipher text output. The output BWMC encryption are 20 bits horizontal bits and 16 bits vertical bits and these two bits data is for error bit detection in decryption sections.

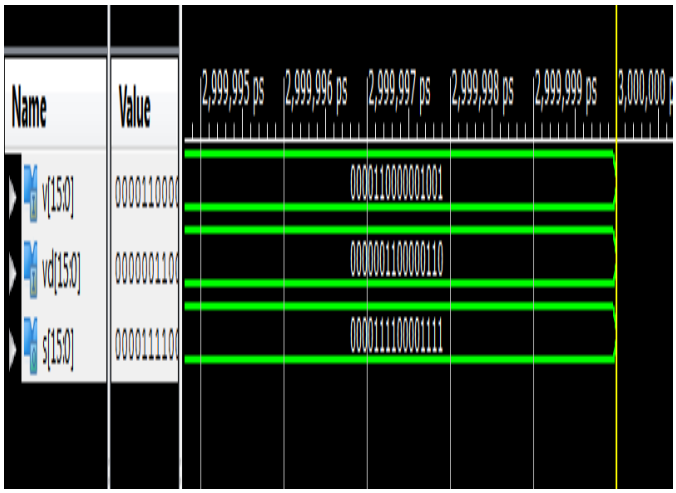


Fig.5. BWMC Decryption output in Xilinx Isim simulator

The vertical bits of encryption module is input to decryption module which includes same of integer operation to get 16 bits syndrome bits for identification of error bit at error locator. The 's' represents in the Fig.5. is the syndrome bits which is performed between XOR operation between 'v' and 'vd' as shown in Fig.5. The horizontal bits of encryption module is input to decryption module which includes same of integer operation to get 16 bits syndrome bits for identification of error bit at error locator. The 'h' represents in the Fig.6. is the syndrome bits which is performed between XOR operation between 'h' and 'hd' as shown in Fig.6. The 'v' and 'h' are inputs to error locator and error detector modules and the outputs of encryption and decryption are shown in the Fig.7. and its RTL diagram is shown in Fig.8.

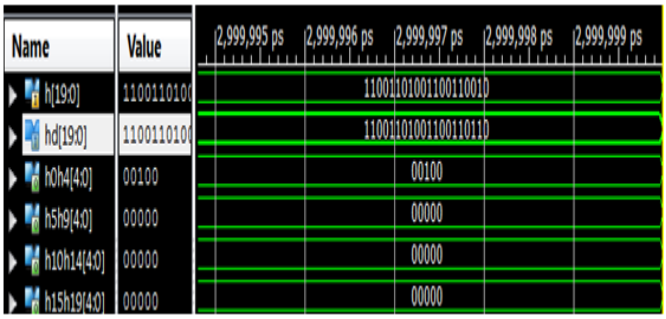


Fig.6. Output of BWMC detector

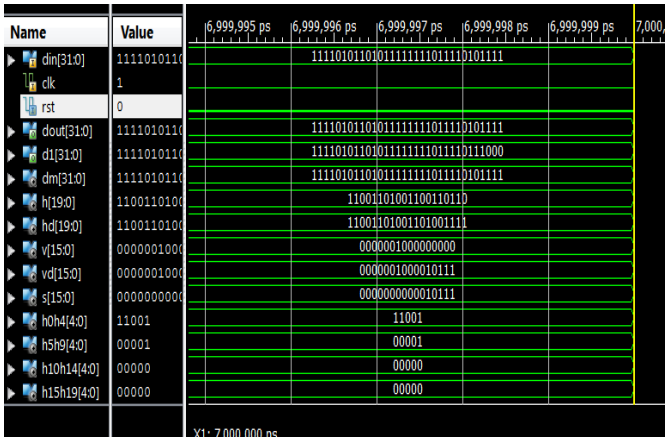


Fig.7.Output of BWMCencryption and decryption

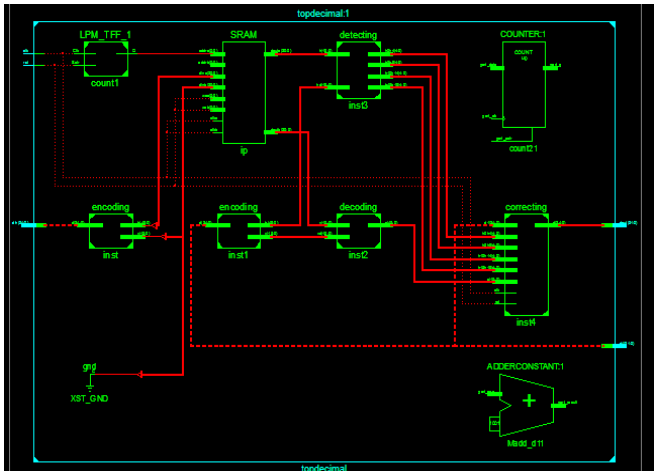


Fig.8. Top module RTL Schematic of BWMC encryption and decryption

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

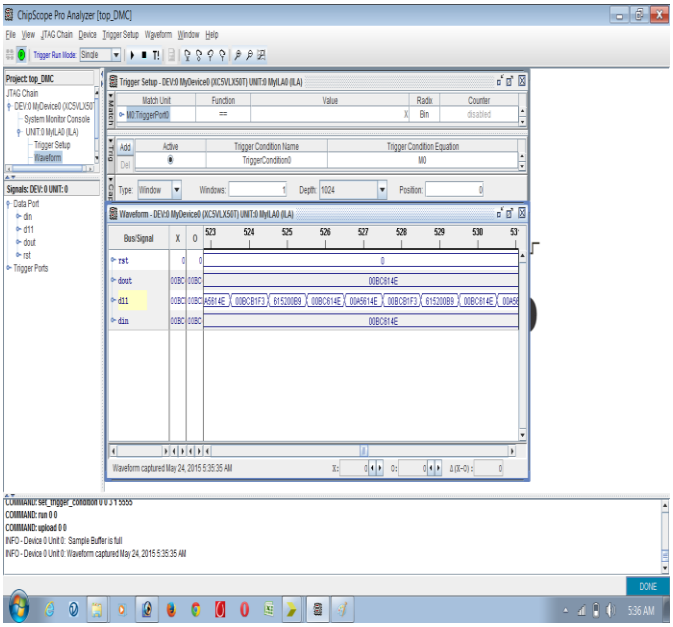


Fig.9. BWMC encryption and decryption Vertex-5 hardware FPGA output using Cadence tool

The proposed cryptography system is validated and verified in terms timing and encryption and decryption processes in Viertex-5 FPGA using Chipscope Pro tool in Xilinx 14.7 ISE tool and each stage of outputs are shown in Fig.9. The Xilinx 14.7 ISE tool provides only dynamic values of power, delay and hardware resources so the proposed work is also validated in Cadence 45nm Technology tool to calculate exact power, delay and utilization of resources in terms of flip flops, number slices, LUT's and memory utilization. The Fig.10.shows the elaborated RTL diagram for Bitwise matrix code extracted using RC compiler in Cadence digital tool. The RTL diagram of detector circuit in decryption of BWMC is shown in Fig.11. In the decryption process, there are four different stages to decrypt the original data, the third stage is corrector to correct the corrupted bits using XOR operation discussed in equation (12) and its RTL diagram in terms of LUT is shown in Fig.12. and LUT with delay flip flops is shown in Fig.13. The overall RTL diagram of encryption and decryption of BWMC is shown in Fig.14. and its consists of XOR operation, syndrome calculator, error locator, error detector and error corrector modules.

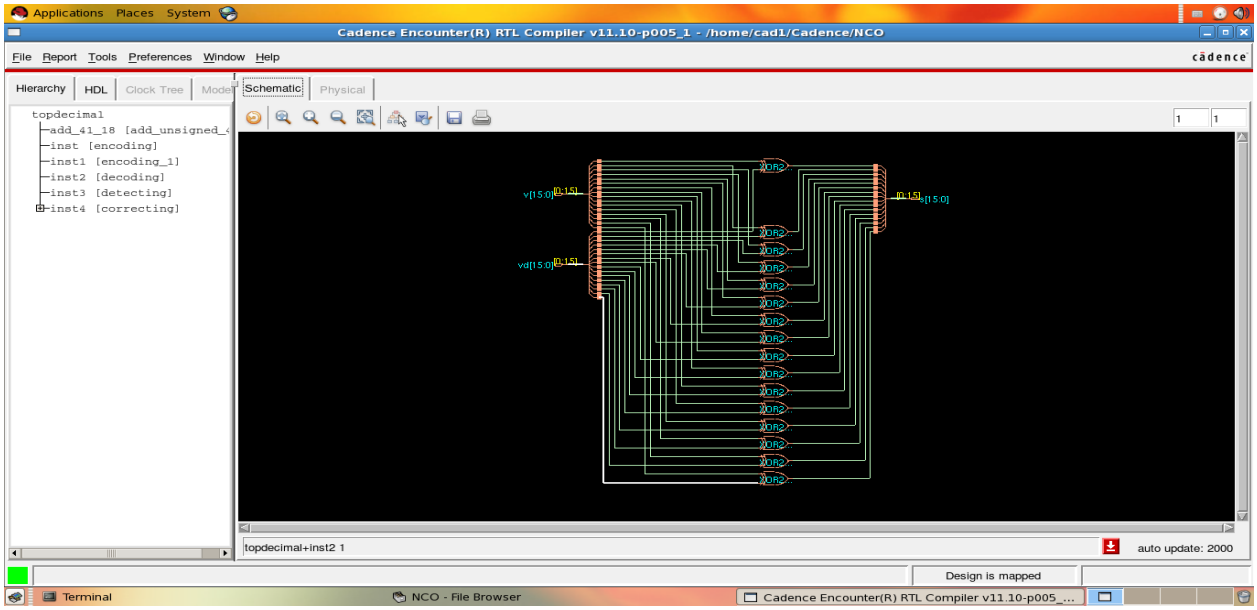


Fig.10. RTL diagram of BWMC encryption output using Cadence tool

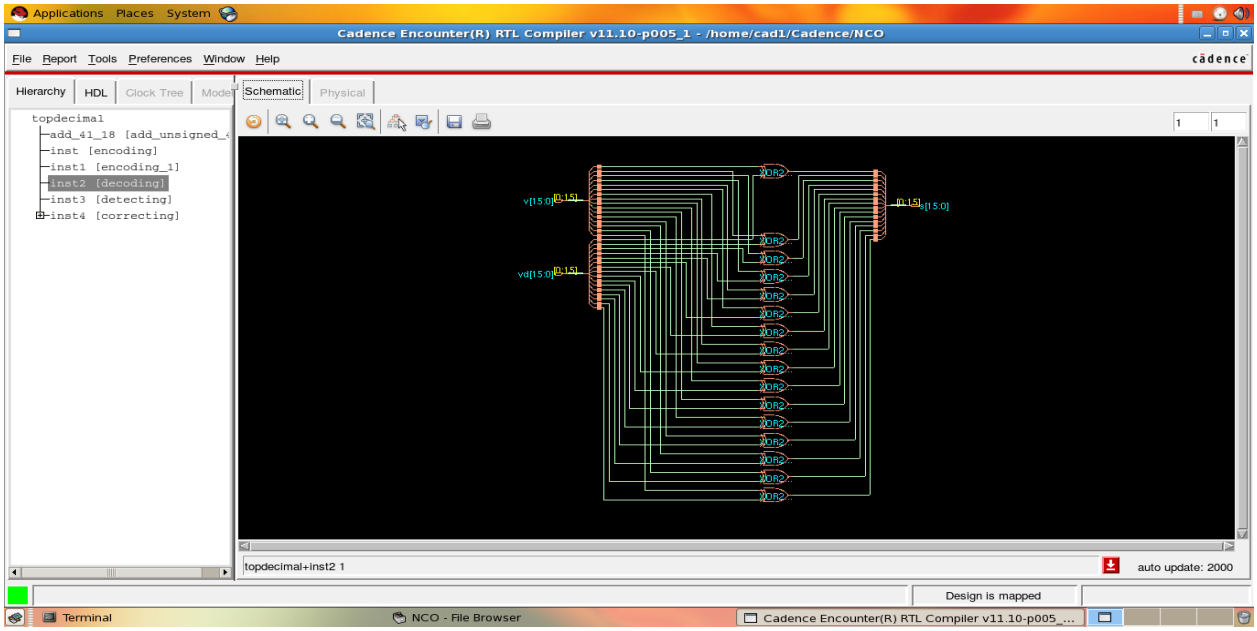


Fig.11. RTL diagram of Detector module Output using RC encounter Cadence tool

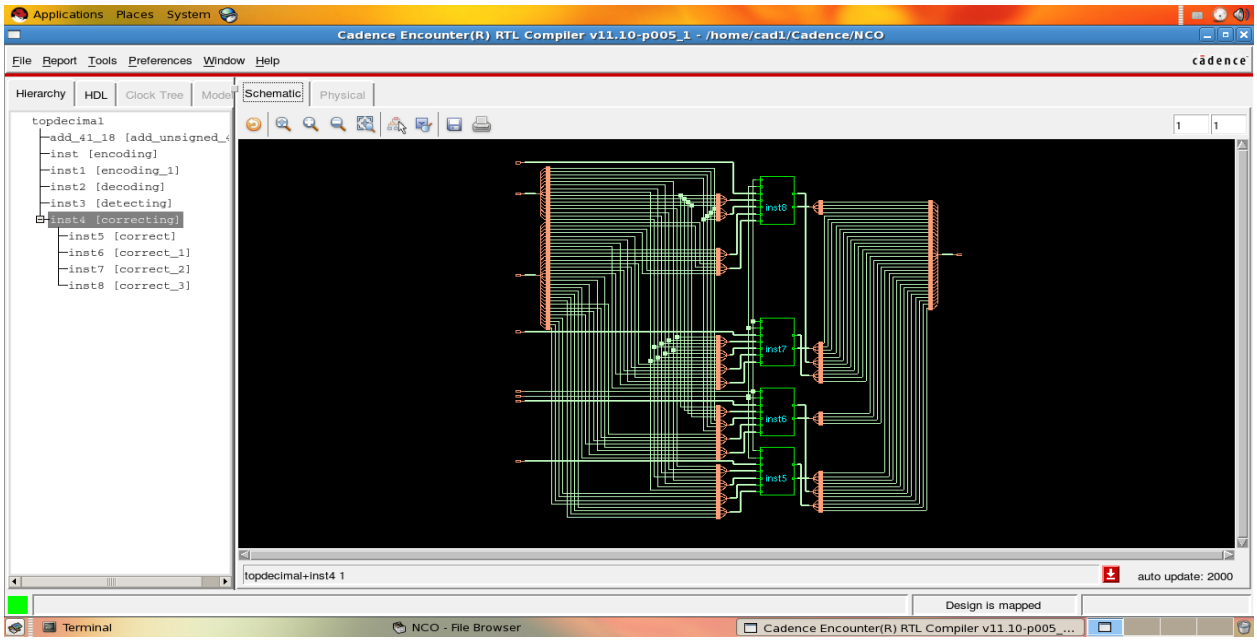


Fig.12. RTL diagram of corrector moduleoutput using RC encounter Cadence tool in terms LUT's

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

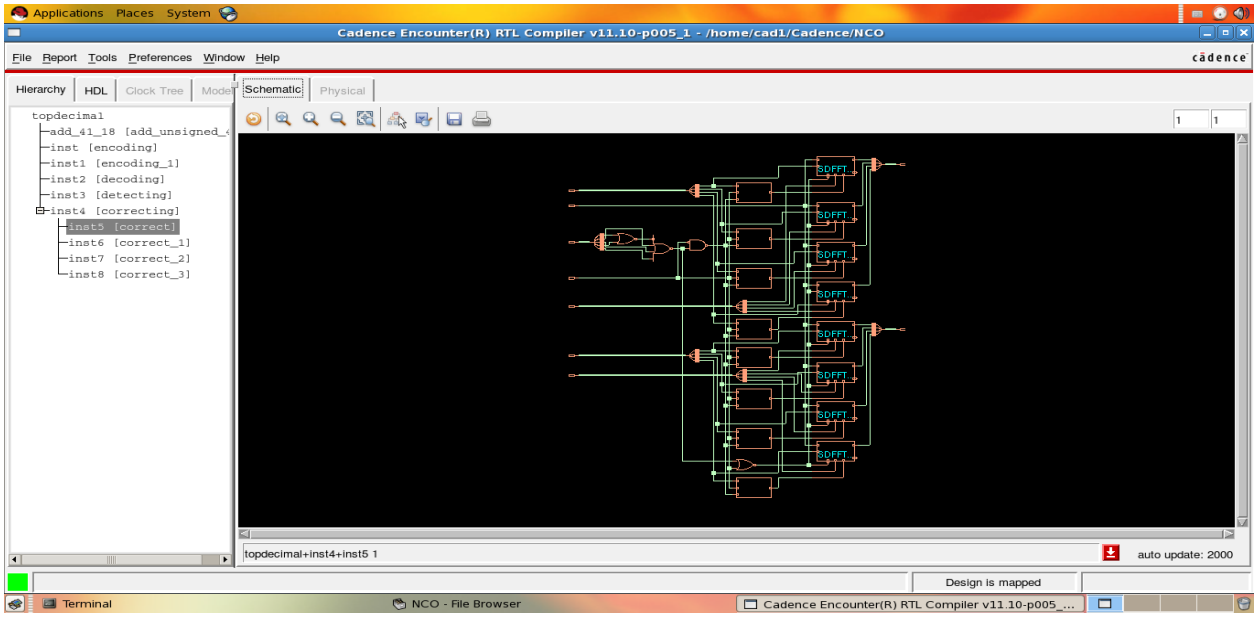


Fig.13. RTL diagram of internal corrector module output using RC encounter Cadence tool

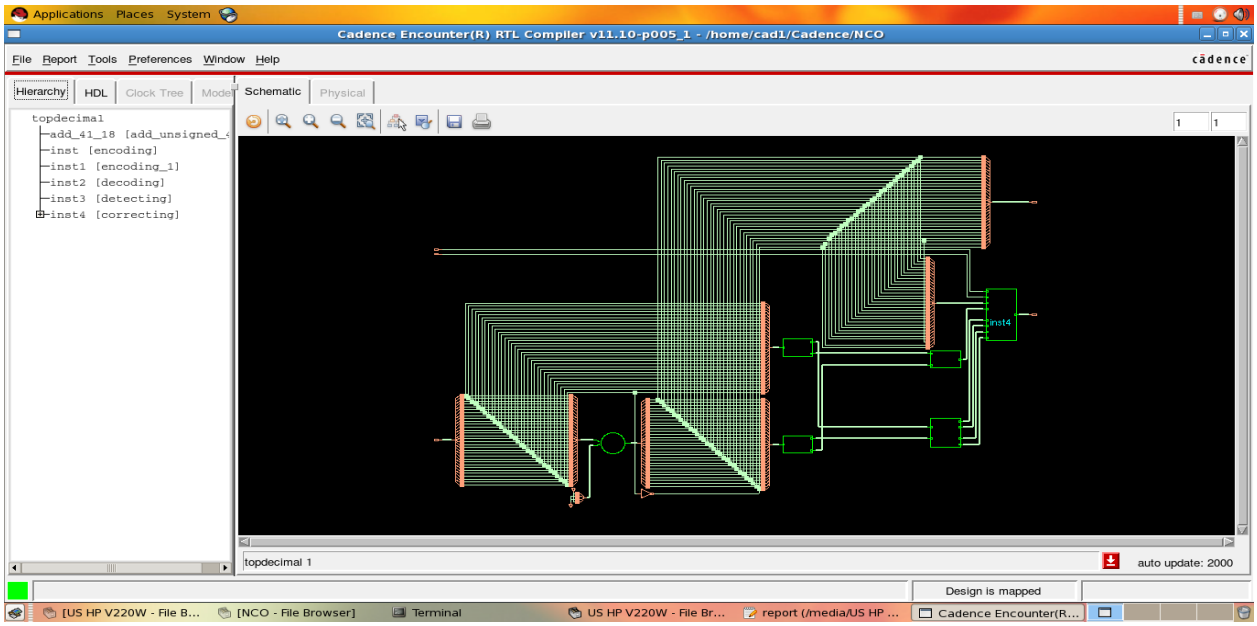


Fig.14. Top RTL diagram of BWMC encryption and decryption using RC encounter Cadence tool

The encrypted data has 20 bits horizontal and 16 bits vertical which are generated from integer addition and XOR operation and these will be used in decryption stage as check bits. These check bits are applied for integer addition and XOR operation again for generation of different symbols of syndrome symbol s, each 5 bits. Using error locator module, the error bit will be identified in each symbol. The corrupted bits are corrected using XOR operation between horizontal, vertical and symbol bits and its equation is shown in 12

$$D_{correct} = D_{[i]} \oplus S_{[i]} - - - - 12$$

Where I is the integer number varies from 0 to 4

The equation 11will be used for 8 times because input data size is 32 bits it includes x,y, and secrete character so 32/4 bits is gives 8 symbols and each symbol is 5 bits. The last stage is decryption is rearrangement of ECC point which has x,y, and secrete character. The proposed work is designed in Verilog HDL and validated on Virtex-5 FPGA HDL using Chipscope pro analyzer tool which is integrated with Xilinx 14.7 ISE. The complete work also verified in Cadence software tool of 180nm technology to obtained the total power and it is sum of static and dynamic powers and using RC encounter in Cadence tool the chip level design and RTL diagram for each stages are generated and shown in Fig.13 and 14 and the decrypted data of 32 bits are successfully decoded and result of 32 bits is shown in Fig.15.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

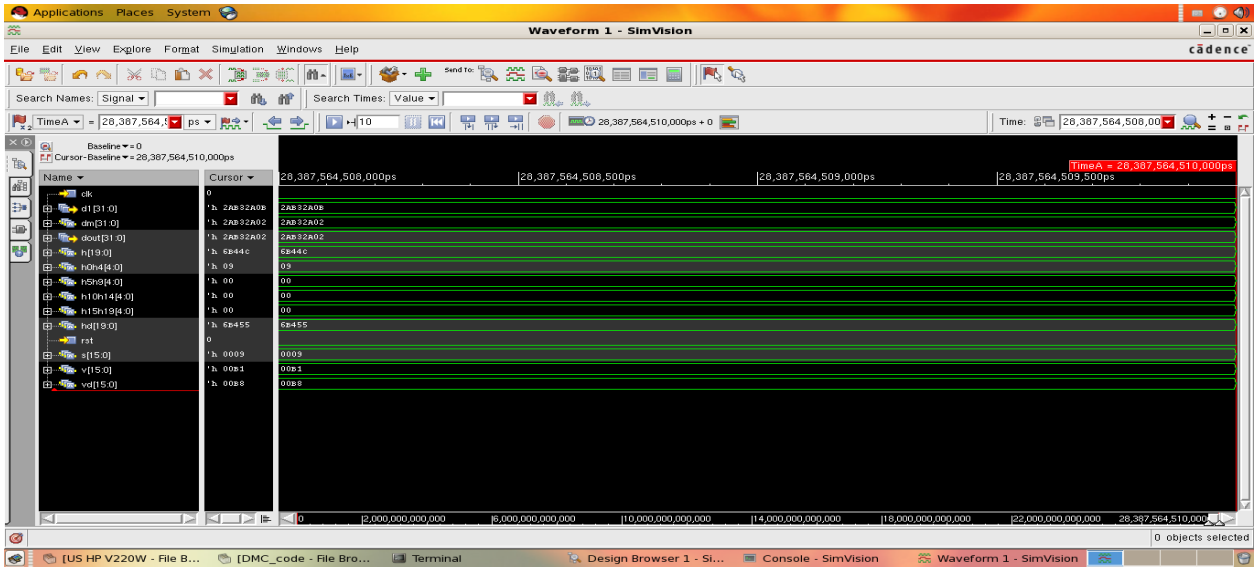


Fig.15. BWMC encryption and decryption simulation results using RC compiler Cadence tool

V. CONCLUSION

The encoder, decoder and ECC cryptography are presented in this paper to map any characters and numbers into ECC points. The mapped points are encoded using BWMC encoder and then transmitted through wireless media and at the receiver section, the data is decoded by using syndromes calculation, error detection and error correction techniques. The results obtained from BWMC encoder is completely eliminatedthrough the regularity and therefore decoding the data without errors is improved. Hence, hacking the data between the sender and the receiver by intrudes would be very difficult to find on which point the data is mapped. Thus, it is concluded that the BWMC encoder and decoder along with ECC techniques are more secure and more confidential and also it is memory error free. The ECC and other techniques used in this work are different in utilization of error events; further corrected the distinguished ones. Conversely the fault discovery capacity and the expensesare differing in view of the codes utilized. The proposed BWMC system achieves in detecting and correcting the errors very efficiently using the bitwise matrix code algorithm method. In comparison to previous works the Enhanced BWMC have the capability to correct errors up to 5 bits in a symbol. The proposed system shows that it has a superior protection levelcompared to the large multiple cell upsets in the memory cells. The BWMC results are compared in terms of mean time to failure with existing techniques like MC's, difference in punctured set, hamming codes and found to be BWMC along with ECC produces the better results. The proposed work improved in terms of delay i.e. 73.1% as compared with hamming, 69% improvement as compared with MC's.

REFERENCE

1. Arunkumar, Dr. S.S. Tyagi, ManishaRana, NehaAggarwal, PawanBhadana, ManavRachna (2011), A Comparative Study of Public Key Cryptosystem based on ECC and RSA. *International Journal on Computer Science and Engineering (IJCSE)*, ISSN : 0975-3397 Vol. 3 No. 5 May 2011, 1904-1909.
2. O. Srinivasa Rao (2010), Efficient Mapping Methods For Elliptic Curve Cryptosystems. *International Journal of Engineering Science and Technology*, Vol. 2(8), 2010, ISSN: 0975-5462, 3651-3656
3. C. Wang, M. Daneshmand, M. Dohler, X. Mao, R. Q. Hu and H. Wang (2013), Guest Editorial - Special Issue on Internet of Things (IoT): Architecture, Protocols and Services". *IEEE Sensors Journal*, vol. 13, issue. 10, pp. 3505–3510.
4. S. Raza, (2014) Secure communication for the Internet of Things - a comparison of link-layer security and IP sec for 6LoWPAN. *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668.
5. Gonzalez G. Organero M, Kloos C (2008). Early in infrastructure of all Internet of Things in space for learning. *8th IEEE International Conference on Advance Learning Technologies*, pp-381-383.
6. Yanbing Liu, Wenping Hu, Jiang Du (2011), Network Information Security Architecture Based on Internet of Things. *ZTE Communication*, Vol. 17(1):17-20
7. Riaz Naseer and Jeff Draper (2008), "Parallel Double Error Correcting Code Design to Mitigate Multi-Bit Upsets in SRAMs". 978-1-4244-2361-3/08, IEEE.
8. Juan Antonio Maestro, Pedro Reviriego, SanghyeonBaeg, Shijie Wen, Richard Wong (2013), Soft error tolerant Content Addressable Memories (CAMs) using error detection code and duplication. Microprocessors and Microsystems 37 (2013) 1103–1107, 2013 Elsevier B.V. http://dx.doi.org/10.1016/j.micpro.2013.10.003, 0141-9331.
9. Gustavo Neuberger, Fernanda Gusmao de lima, kastensmidt and Ricardo Reis (2005), An Automatic Technique for Optimizing Reed – Solomon Codes to Improve Fault Tolerance in Memories. *IEEE Co-published by the IEEE CS and the IEEE CASS IEEE Design & Test of Computers*, 0740-7475/05
10. Sanghyeon Baeg, Pedro Reviriego, Juan Antonio Maestro, Shijie and Richard Wong (2011), Analysis of a Multiple Cell Upset Failure Model for Memories. *ACM Transactions on Design Automation of Electronic Systems*, Vol. 16, No. 4, Article 45, 1084-4309
11. Sandeep M D and Rajashekhargouda C. Patil (2016), An Approach to Reduce Number of Redundant Bits used To Overcome Cell Upsets in Memory using Decimal Matrix Code. *International Journal of Science, Engineering and Technology Research (IJSETR)*, Volume 5, Issue 5, 200-2010.
12. Costas Argyrides, StephaniaLoizidou and Dhiraj K. Pradhan (2008), Area Reliability Trade – Off in Improved Reed Muller Coding. SAMOS 2008, LNCS 5114, 2008 Springer – Verlag Berlin Heidelber, pp. 116-125.
13. Bertozzi, D., Et Al (2005).: Error Control Schemes For On-Chip Communication Links: The Energy-Reliability Tradeoff. *IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems*, Vol. 24, No. 6.
14. Rossi, D., Metra, C(2003): Error correcting strategy for high speed and density reliable flash memories. *IEEE Journal. Electronic Testing, Theory and applications*, 19(5), 511–521.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

15. Argyrides, C., Pradhan, D.K (2007): Improved Decoding Algorithm for High Reliable Reed Muller Coding. *SAMOS 2008, LNCS 5114*, pp. 116–125, 2008, (Eds.): SAMOS 2008, LNCS 5114, pp. 116–125.
16. R.Balamurugan, V.Kamalakannan, S.Tamilselvan and D.RahulGandh, (2014) "Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography". *International Conference on Contemporary Computing and Informatics (IC3I 2014)*, pp 103-106.
17. Smyth N., McLoone M., McCanny J. V (2006). WLAN Security Processor. *IEEE Transactions on Circuits and Systems* I: Fundamental Theory and Applications, Vol. 53, Issue 7, ISSN: 1057-7122, pp: 1506- 1520.
18. Bae D., Kim G., Kim J., Park S., Song O (2005). An Efficient Design of CCMP for Robust SecurityNetwork. ICISC 2005, *Lecture Notes in Computer Science* 3935, Springer-Berlin,2006, pp. 352-361.
19. Syed Mohsin Abbas (2014), "An Efficient Multiple Cell Upsets Tolerant Content-Addressable Memory", *IEEE Transactions On Computers*, VOL. 63, NO. 8.
20. Fu Minfeng 92010), Elliptic Curve Cryptosystem EIGamal Encryption and Transmission Scheme. *International Conference on Computer Application and System Modeling* (ICCASM 2010), 978-1-4244-7237-6/10, IEEE, 2010.

Appendix-I

Table-I

y	y^2	y^2 mod p	y	y^2	y^2 mod p	y	y^2	y^2 mod p
1	1	1	41	1681	555	81	6561	368
2	4	4	42	1764	75	82	6724	531
3	9	9	43	1849	160	83	6889	133
4	16	16	44	1936	247	84	7056	300
5	25	25	45	2025	336	85	7225	469
6	36	36	46	2116	427	86	7396	77
7	49	49	47	2209	520	87	7569	250
8	64	64	48	2304	52	88	7744	425
9	81	81	49	2401	149	89	7921	39
10	100	100	50	2500	248	90	8100	218
11	121	121	51	2601	349	91	8281	399
12	144	144	52	2704	452	92	8464	19
13	169	169	53	2809	557	93	8649	204
14	196	196	54	2916	101	94	8836	391
15	225	225	55	3025	210	95	9025	17
16	256	256	56	3136	321	96	9216	208
17	289	289	57	3249	434	97	9409	401
18	324	324	58	3364	549	98	9604	33
19	361	361	59	3481	103	99	9801	230
20	400	400	60	3600	222	100	10000	429
21	441	441	61	3721	343	101	10201	67
22	484	484	62	3844	466	102	10404	270
23	529	529	63	3969	28	103	10609	475
24	576	13	64	4096	155	104	10816	119
25	625	62	65	4225	284	105	11025	328
26	676	113	66	4356	415	106	11236	539
27	729	166	67	4489	548	107	11449	189
28	784	221	68	4624	120	108	11664	404
29	841	278	69	4761	257	109	11881	58
30	900	337	70	4900	396	110	12100	277
31	961	398	71	5041	537	111	12321	498
32	1024	461	72	5184	117	112	12544	158
33	1089	526	73	5329	262	113	12769	383
34	1156	30	74	5476	409	114	12996	47

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

35	1225	99	75	5625	558	115	13225	276
36	1296	170	76	5776	146	116	13456	507
37	1369	243	77	5929	299	117	13689	177
38	1444	318	78	6084	454	118	13924	412
39	1521	395	79	6241	48	119	14161	86
40	1600	474	80	6400	207	120	14400	325

y	y^2	y^2 mod p	y	y^2	y^2 mod p	y	y^2	y^2 mod p
121	14641	3	161	25921	23	201	40401	428
122	14884	246	162	26244	346	202	40804	268
123	15129	491	163	26569	108	203	41209	110
124	15376	175	164	26896	435	204	41616	517
125	15625	424	165	27225	201	205	42025	363
126	15876	112	166	27556	532	206	42436	211
127	16129	365	167	27889	302	207	42849	61
128	16384	57	168	28224	74	208	43264	476
129	16641	314	169	28561	411	209	43681	330
130	16900	10	170	28900	187	210	44100	186
131	17161	271	171	29241	528	211	44521	44
132	17424	534	172	29584	308	212	44944	467
133	17689	236	173	29929	90	213	45369	329
134	17956	503	174	30276	437	214	45796	193
135	18225	209	175	30625	223	215	46225	59
136	18496	480	176	30976	11	216	46656	490
137	18769	190	177	31329	364	217	47089	360
138	19044	465	178	31684	156	218	47524	232
139	19321	179	179	32041	513	219	47961	106
140	19600	458	180	32400	309	220	48400	545
141	19881	176	181	32761	107	221	48841	423
142	20164	459	182	33124	470	222	49284	303
143	20449	181	183	33489	272	223	49729	185
144	20736	468	184	33856	76	224	50176	69
145	21025	194	185	34225	445	225	50625	518
146	21316	485	186	34596	253	226	51076	406
147	21609	215	187	34969	63	227	51529	296
148	21904	510	188	35344	438	228	51984	188
149	22201	244	189	35721	252	229	52441	82
150	22500	543	190	36100	68	230	52900	541
151	22801	281	191	36481	449	231	53361	439
152	23104	21	192	36864	269	232	53824	339
153	23409	326	193	37249	91	233	54289	241
154	23716	70	194	37636	478	234	54756	145
155	24025	379	195	38025	304	235	55225	51
156	24336	127	196	38416	132	236	55696	522
157	24649	440	197	38809	525	237	56169	432
158	24964	192	198	39204	357	238	56644	344
159	25281	509	199	39601	191	239	57121	258

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

160	25600	265	200	40000	27	240	57600	174
y	y^2	y^2 mod p	y	y^2	y^2 mod p	y	y^2	y^2 mod p
241	58081	92	281	78961	141	321	103041	12
242	58564	12	282	79524	141	322	103684	92
243	59049	497	283	80089	143	323	104329	174
244	59536	421	284	80656	147	324	104976	258
245	60025	347	285	81225	153	325	105625	344
246	60516	275	286	81796	161	326	106276	432
247	61009	205	287	82369	171	327	106929	522
248	61504	137	288	82944	183	328	107584	51
249	62001	71	289	83521	197	329	108241	145
250	62500	7	290	84100	213	330	108900	241
251	63001	508	291	84681	231	331	109561	339
252	63504	448	292	85264	251	332	110224	439
253	64009	390	293	85849	273	333	110889	541
254	64516	334	294	86436	297	334	111556	82
255	65025	280	295	87025	323	335	112225	188
256	65536	228	296	87616	351	336	112896	296
257	66049	178	297	88209	381	337	113569	406
258	66564	130	298	88804	413	338	114244	518
259	67081	84	299	89401	447	339	114921	69
260	67600	40	300	90000	483	340	115600	185
261	68121	561	301	90601	521	341	116281	303
262	68644	521	302	91204	561	342	116964	423
263	69169	483	303	91809	40	343	117649	545
264	69696	447	304	92416	84	344	118336	106
265	70225	413	305	93025	130	345	119025	232
266	70756	381	306	93636	178	346	119716	360
267	71289	351	307	94249	228	347	120409	490
268	71824	323	308	94864	280	348	121104	59
269	72361	297	309	95481	334	349	121801	193
270	72900	273	310	96100	390	350	122500	329
271	73441	251	311	96721	448	351	123201	467
272	73984	231	312	97344	508	352	123904	44
273	74529	213	313	97969	7	353	124609	186
274	75076	197	314	98596	71	354	125316	330
275	75625	183	315	99225	137	355	126025	476
276	76176	171	316	99856	205	356	126736	61
277	76729	161	317	100489	275	357	127449	211
278	77284	153	318	101124	347	358	128164	363
279	77841	147	319	101761	421	359	128881	517
280	78400	143	320	102400	497	360	129600	110

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

y	y^2	y^2 mod p	y	y^2	y^2 mod p	y	y^2	y^2 mod p
361	130321	268	401	160801	346	441	194481	246
362	131044	428	402	161604	23	442	195364	3
363	131769	27	403	162409	265	443	196249	325
364	132496	191	404	163216	509	444	197136	86
365	133225	357	405	164025	192	445	198025	412
366	133956	525	406	164836	440	446	198916	177
367	134689	132	407	165649	127	447	199809	507
368	135424	304	408	166464	379	448	200704	276
369	136161	478	409	167281	70	449	201601	47
370	136900	91	410	168100	326	450	202500	383
371	137641	269	411	168921	21	451	203401	158
372	138384	449	412	169744	281	452	204304	498
373	139129	68	413	170569	543	453	205209	277
374	139876	252	414	171396	244	454	206116	58
375	140625	438	415	172225	510	455	207025	404
376	141376	63	416	173056	215	456	207936	189
377	142129	253	417	173889	485	457	208849	539
378	142884	445	418	174724	194	458	209764	328
379	143641	76	419	175561	468	459	210681	119
380	144400	272	420	176400	181	460	211600	475
381	145161	470	421	177241	459	461	212521	270
382	145924	107	422	178084	176	462	213444	67
383	146689	309	423	178929	458	463	214369	429
384	147456	513	424	179776	179	464	215296	230
385	148225	156	425	180625	465	465	216225	33
386	148996	364	426	181476	190	466	217156	401
387	149769	11	427	182329	480	467	218089	208
388	150544	223	428	183184	209	468	219024	17
389	151321	437	429	184041	503	469	219961	391
390	152100	90	430	184900	236	470	220900	204
391	152881	308	431	185761	534	471	221841	19
392	153664	528	432	186624	271	472	222784	399
393	154449	187	433	187489	10	473	223729	218
394	155236	411	434	188356	314	474	224676	39
395	156025	74	435	189225	57	475	225625	425
396	156816	302	436	190096	365	476	226576	250
397	157609	532	437	190969	112	477	227529	77
398	158404	201	438	191844	424	478	228484	469
399	159201	435	439	192721	175	479	229441	300
400	160000	108	440	193600	491	480	230400	133

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

y	y^2	y^2 mod p	y	y^2	y^2 mod p	y	y^2	y^2 mod p
481	231361	531	521	271441	75	561	314721	4
482	232324	368	522	272484	555	562	315844	1
483	233289	207	523	273529	474	563	316969	0
484	234256	48	524	274576	395			
485	235225	454	525	275625	318			
486	236196	299	526	276676	243			
487	237169	146	527	277729	170			
488	238144	558	528	278784	99			
489	239121	409	529	279841	30			
490	240100	262	530	280900	526			
491	241081	117	531	281961	461			
492	242064	537	532	283024	398			
493	243049	396	533	284089	337			
494	244036	257	534	285156	278			
495	245025	120	535	286225	221			
496	246016	548	536	287296	166			
497	247009	415	537	288369	113			
498	248004	284	538	289444	62			
499	249001	155	539	290521	13			
500	250000	28	540	291600	529			
501	251001	466	541	292681	484			
502	252004	343	542	293764	441			
503	253009	222	543	294849	400			
504	254016	103	544	295936	361			
505	255025	549	545	297025	324			
506	256036	434	546	298116	289			
507	257049	321	547	299209	256			
508	258064	210	548	300304	225			
509	259081	101	549	301401	196			
510	260100	557	550	302500	169			
511	261121	452	551	303601	144			
512	262144	349	552	304704	121			
513	263169	248	553	305809	100			
514	264196	149	554	306916	81			
515	265225	52	555	308025	64			
516	266256	520	556	309136	49			
517	267289	427	557	310249	36			
518	268324	336	558	311364	25			
519	269361	247	559	312481	16			
520	270400	160	560	313600	9			

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table-II

Annexure-II

x	x^3	Q	Q1	x	x^3	Q	Q1	x	x^3	Q	Q1
121	1771561	1771562	364	161	4173281	4173282	326	201	8120601	8120602	453
122	1815848	1815849	174	162	4251528	4251529	316	202	8242408	8242409	89
123	1860867	1860868	153	163	4330747	4330748	152	203	8365427	8365428	374
124	1906624	1906625	307	164	4410944	4410945	403	204	8489664	8489665	188
125	1953125	1953126	79	165	4492125	4492126	512	205	8615125	8615126	100
126	2000376	2000377	38	166	4574296	4574297	485	206	8741816	8741817	116
127	2048383	2048384	190	167	4657463	4657464	328	207	8869743	8869744	242
128	2097152	2097153	541	168	4741632	4741633	47	208	8998912	8998913	484
129	2146689	2146690	534	169	4826809	4826810	211	209	9129329	9129330	285
130	2197000	2197001	175	170	4913000	4913001	263	210	9261000	9261001	214
131	2248091	2248092	33	171	5000211	5000212	209	211	9393931	9393932	277
132	2299968	2299969	114	172	5088448	5088449	55	212	9528128	9528129	480
133	2352637	2352638	424	173	5177717	5177718	370	213	9663597	9663598	266
134	2406104	2406105	406	174	5268024	5268025	34	214	9800344	9800345	204
135	2460375	2460376	66	175	5359375	5359376	179	215	9938375	9938376	300
136	2515456	2515457	536	176	5451776	5451777	248	216	10077696	10077697	560
137	2571353	2571354	133	177	5545233	5545234	247	217	10218313	10218314	427
138	2628072	2628073	552	178	5639752	5639753	182	218	10360232	10360233	470
139	2685619	2685620	110	179	5735339	5735340	59	219	10503459	10503460	132
140	2744000	2744001	502	180	5832000	5832001	447	220	10648000	10648001	545
141	2803221	2803222	45	181	5929741	5929742	226	221	10793861	10793862	26
142	2863288	2863289	434	182	6028568	6028569	528	222	10941048	10941049	270
143	2924207	2924208	549	183	6128487	6128488	233	223	11089567	11089568	157
144	2985984	2985985	396	184	6229504	6229505	473	224	11239424	11239425	256
145	3048625	3048626	544	185	6331625	6331626	128	225	11390625	11390626	10
146	3112136	3112137	436	186	6434856	6434857	330	226	11543176	11543177	551
147	3176523	3176524	78	187	6539203	6539204	522	227	11697083	11697084	196
148	3241792	3241793	39	188	6644672	6644673	147	228	11852352	11852353	77
149	3307949	3307950	325	189	6751269	6751270	337	229	12008989	12008990	200
150	3375000	3375001	379	190	6859000	6859001	535	230	12167000	12167001	8
151	3442951	3442952	207	191	6967871	6967872	184	231	12326391	12326392	70
152	3511808	3511809	378	192	7077888	7077889	416	232	12487168	12487169	392
153	3581577	3581578	335	193	7189057	7189058	111	233	12649337	12649338	417
154	3652264	3652265	84	194	7301384	7301385	401	234	12812904	12812905	151
155	3723875	3723876	194	195	7414875	7414876	166	235	12977875	12977876	163
156	3796416	3796417	108	196	7529536	7529537	538	236	13144256	13144257	459
157	3869893	3869894	395	197	7645373	7645374	397	237	13312053	13312054	482
158	3944312	3944313	498	198	7762392	7762393	312	238	13481272	13481273	238
159	4019679	4019680	423	199	7880599	7880600	289	239	13651919	13651920	296
160	4096000	4096001	176	200	8000000	8000001	334	240	13824000	13824001	99

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

x	x^3	Q	Q1	x	x^3	Q	Q1	x	x^3	Q	Q1
241	13997521	13997522	216	281	22188041	22188042	212	321	33076161	33076162	475
242	14172488	14172489	90	282	22425768	22425769	353	322	33386248	33386249	349
243	14348907	14348908	290	283	22665187	22665188	497	323	33698267	33698268	466
244	14526784	14526785	259	284	22906304	22906305	87	324	34012224	34012225	269
245	14706125	14706126	3	285	23149125	23149126	255	325	34328125	34328126	327
246	14886936	14886937	91	286	23393656	23393657	444	326	34645976	34645977	83
247	15069223	15069224	529	287	23639903	23639904	97	327	34965783	34965784	106
248	15252992	15252993	197	288	23887872	23887873	346	328	35287552	35287553	402
249	15438249	15438250	227	289	24137569	24137570	71	329	35611289	35611290	414
250	15625000	15625001	62	290	24389000	24389001	404	330	35937000	35937001	148
251	15813251	15813252	271	291	24642171	24642172	225	331	36264691	36264692	173
252	16003008	16003009	297	292	24897088	24897089	103	332	36594368	36594369	495
253	16194277	16194278	146	293	25153757	25153758	44	333	36926037	36926038	557
254	16387064	16387065	387	294	25412184	25412185	54	334	37259704	37259705	365
255	16581375	16581376	463	295	25672375	25672376	139	335	37595375	37595376	488
256	16777216	16777217	380	296	25934336	25934337	305	336	37933056	37933057	369
257	16974593	16974594	144	297	26198073	26198074	558	337	38272753	38272754	14
258	17173512	17173513	324	298	26463592	26463593	341	338	38614472	38614473	555
259	17373979	17373980	363	299	26730899	26730900	223	339	38958219	38958220	309
260	17576000	17576001	267	300	27000000	27000001	210	340	39304000	39304001	408
261	17779581	17779582	42	301	27270901	27270902	308	341	39651821	39651822	295
262	17984728	17984729	257	302	27543608	27543609	523	342	40001688	40001689	539
263	18191447	18191448	355	303	27818127	27818128	298	343	40353607	40353608	20
264	18399744	18399745	342	304	28094464	28094465	202	344	40707584	40707585	433
265	18609625	18609626	224	305	28372625	28372626	241	345	41063625	41063626	95
266	18821096	18821097	7	306	28652616	28652617	421	346	41421736	41421737	138
267	19034163	19034164	260	307	28934443	28934444	185	347	41781923	41781924	5
268	19248832	19248833	426	308	29218112	29218113	102	348	42144192	42144193	265
269	19465109	19465110	511	309	29503629	29503630	178	349	42508549	42508550	361
270	19683000	19683001	521	310	29791000	29791001	419	350	42875000	42875001	299
271	19902511	19902512	462	311	30080231	30080232	268	351	43243551	43243552	85
272	20123648	20123649	340	312	30371328	30371329	294	352	43614208	43614209	288
273	20346417	20346418	161	313	30664297	30664298	503	353	43986977	43986978	351
274	20570824	20570825	494	314	30959144	30959145	338	354	44361864	44361865	280
275	20796875	20796876	219	315	31255875	31255876	368	355	44738875	44738876	81
276	21024576	21024577	468	316	31554496	31554497	36	356	45118016	45118017	323
277	21253933	21253934	121	317	31855013	31855014	474	357	45499293	45499294	449
278	21484952	21484953	310	318	32157432	32157433	562	358	45882712	45882713	465
279	21717639	21717640	478	319	32461759	32461760	306	359	46268279	46268280	377
280	21952000	21952001	68	320	32768000	32768001	275	360	46656000	46656001	191

x	x^3	Q	Q1	x	x^3	Q	Q1	x	x^3	Q	Q1
361	47045881	47045882	476	401	64481201	64481202	249	441	85766121	85766122	391
362	47437928	47437929	112	402	64964808	64964809	239	442	86350888	86350889	201
363	47832147	47832148	231	403	65450827	65450828	389	443	86938307	86938308	411

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

364	48228544	48228545	276	404	65939264	65939265	142	444	87528384	87528385	464
365	48627125	48627126	253	405	66430125	66430126	67	445	88121125	88121126	366
366	49027896	49027897	168	406	66923416	66923417	170	446	88716536	88716537	123
367	49430863	49430864	27	407	67419143	67419144	457	447	89314623	89314624	304
368	49836032	49836033	399	408	67917312	67917313	371	448	89915392	89915393	352
369	50243409	50243410	164	409	68417929	68417930	481	449	90518849	90518850	273
370	50653000	50653001	454	410	68921000	68921001	230	450	91125000	91125001	73
371	51064811	51064812	149	411	69426531	69426532	187	451	91733851	91733852	321
372	51478848	51478849	381	412	69934528	69934529	358	452	92345408	92345409	460
373	51895117	51895118	30	413	70444997	70444998	186	453	92959677	92959678	496
374	52313624	52313625	228	414	70957944	70957945	240	454	93576664	93576665	435
375	52734375	52734376	418	415	71473375	71473376	526	455	94196375	94196376	283
376	53157376	53157377	43	416	71991296	71991297	487	456	94818816	94818817	46
377	53582633	53582634	235	417	72511713	72511714	129	457	95443993	95443994	293
378	54010152	54010153	437	418	73034632	73034633	21	458	96071912	96071913	467
379	54439939	54439940	92	419	73560059	73560060	169	459	96702579	96702580	11
380	54872000	54872001	332	420	74088000	74088001	16	460	97336000	97336001	57
381	55306341	55306342	37	421	74618461	74618462	131	461	97972181	97972182	48
382	55742968	55742969	339	422	75151448	75151449	520	462	98611128	98611129	553
383	56181887	56181888	118	423	75686967	75686968	63	463	99252847	99252848	452
384	56623104	56623105	506	424	76225024	76225025	455	464	99897344	99897345	314
385	57066625	57066626	383	425	76765625	76765626	13	465	100544625	100544626	145
386	57512456	57512457	318	426	77308776	77308777	432	466	101194696	101194697	514
387	57960603	57960604	317	427	77854483	77854484	29	467	101847563	101847564	301
388	58411072	58411073	386	428	78402752	78402753	499	468	102503232	102503233	75
389	58863869	58863870	531	429	78953589	78953590	159	469	103161709	103161710	405
390	59319000	59319001	195	430	79507000	79507001	141	470	103823000	103823001	171
391	59776471	59776472	510	431	80062991	80062992	451	471	104487111	104487112	505
392	60236288	60236289	356	432	80621568	80621569	532	472	105154048	105154049	287
393	60698457	60698458	302	433	81182737	81182738	390	473	105823817	105823818	86
394	61162984	61162985	354	434	81746504	81746505	31	474	106496424	106496425	471
395	61629875	61629876	518	435	82312875	82312876	24	475	107171875	107171876	322
396	62099136	62099137	237	436	82881856	82881857	375	476	107850176	107850177	208
397	62570773	62570774	80	437	83453453	83453454	527	477	108531333	108531334	135
398	63044792	63044793	53	438	84027672	84027673	486	478	109215352	109215353	109
399	63521199	63521200	162	439	84604519	84604520	258	479	109902239	109902240	136
400	64000000	64000001	413	440	85184000	85184001	412	480	110592000	110592001	222

Note: $Q=x^3+x+1$ and $Q1=(x^3+x+1) \bmod p$ where $p=563$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)