International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Design and Implementation of High Security Cryptography for Network Applications by Using Bit Transition Encoder and Decoder

M. Indrasena Reddy, A.P. Siva Kumar

Abstract*: *As of late, the security for any data transmission through any channel or media is significant issue because of hacking diverse strategies. Presently a day, rather than giving the security level to data, the improvement is expanded towards the commandeering of data amongst sender and beneficiary. The level of security relying upon the extent of synchronous key which is utilized for encoder and decoder handling and in existing strategies like AES, reed Solomon codes and square codes utilizes the bigger key size yet at the same time there is security issues because of hacking techniques. To address the security level and hacking issues, the novel Bit Transition Encoder and Decoder (BTED) is displayed and synchronous key is created utilizing scalar duplication which incorporates point multiplying and point expansion. The produced focuses are encoded utilizing BTED before transmission and transmitted through remote channel and the encoded information is unravels at collector utilizing BTED with converse operation. The whole novel cryptography framework has been created utilizing mat lab; the outlined framework is tried as far as speed, deferral and control and furthermore approved on Mat lab 2014a.

Keywords*: *Cryptography, ECC, Point addition, point doubling, Security system and BTED.

I. INTRODUCTION

Since, the innovation is becoming quicker, the exploration researchers and businesses are endeavoring to locate the some answer for keep away from the hacking if data. To make more secure the information to exchange through correspondence media, the ECC cryptography is best arrangement and it is more secure among all others cryptography frameworks [26, 27]. The ECC produces the diverse sizes of keys and furthermore manages encryption and decoding for a given information and ECC utilizes both private and open key cryptography. Be that as it may, people in general key cryptography framework gives more secure, accordingly ECC is one such cryptography strategy. The fundamental favorable position of ECC over RSA is that ECC is bolsters even little key to bigger key sizes depending the applications and necessities consequently the handling many-sided quality will be lessened [1]. The point expansion, point multiplying and scalar augmentations are fundamental operations of ECC to discover focuses on the bend. These point operation are helps for playing out the encryption and unscrambling operations. The Elgamal strategy is one of such point operation which is a piece of ECC operation and it likewise bolster for static like coordinated and dynamical like one to N mapping techniques clarified in [2]. In mapping strategy, the alphanumeric characters and numbers are mapped progressively on to the x-y organizers it is exceptionally troublesome for gatecrasher to figure the mapped character or number, henceforth the mapped technique is adjusted regarding framework is called grid mapping technique and it is ensure the security for the information and furthermore keeps away from consistency in the scrambled information. The issues of cryptography framework to trade the data between sender/transmitter and recipient/client can be limited utilizing ECC diffie-hellmen-Merkle key trade by performing scalar augmentation to create the focuses like P, 2P,3P,4P,… … .563P. The created guide P=f(x,y), toward get the 563 focuses, the point expansion and point multiplying are utilized and these procedures will keeps away from complex math operation like increase and divisions accordingly the unpredictability of framework is decreased and speed can be moved forward. The sender message utilizing Elgamal strategy and reed Solomon codes to accelerate the procedure with transmission speed of 200Mbits/sec[3]. The transmitted registers the message into (M+M_s*(M_R*G)), where M is message, M_s is sender message, M_R is recipient message and G is generator point and the message which is encoded by (M_s*G,M+M_S*(M_R*G)) and recollections blunder adjustments introduced in [4]. The sender key KR and registers K_R*(M_s*G) and recipient decodes the information with unique key M by utilizing M+M_s*(M_R*G)- K_R*(M_s*G) in [5] and it is high unwavering quality and decrease excess bits in memory gadgets. For NoC and SoC gadget required rapid and decreased excess operations and these outlines are direct and piece codes displayed in [6]. The various bits mistake amendment, delicate blunders resistance gadget like Content Addressable Memories (CAMs) and delicate mistakes remedies for recollections like SRAM and others recollections gadgets have been proposed in [7].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
M Indrasena reedy*, Department of Computer Science & Engineering, Research Schlor, Jawaharlal Nehru Technological University, Anantapur, India.
Dr. A.P Siva Kumar, Department of Computer Science & Engineering, Jawaharlal Nehru Technological University, Anantapur, India.

The information exchange exchanging gadgets like NoC and SoC frameworks requires the blunders adjustment strategies to disentangle the information at beneficiary and successfully control of information move is exhibited in [8]. The ElGamal and Menezes ECC systems has major difference in terms of points representation for the characters and it consumes less power and high speed in FPGA and ASIC design and the fields are represented over the curve are $F_p.F_p$ [22]. The ECC concept have been invented by the great mathematics in few century, elliptical curves plays a major role in cryptography which uses number theory and security level systems [17]. The ECC concept has been used in factorization of integer numbers and it is very significant in solving the Fermat's theorem proposed in [18]. In 1985, the ECC was invented by Koblitz and Miller [12,29] and it is essentially using for secrete key generation to have high security and it is commercial available in market, the curve w.r.t P is point on the curve and represented by $p(x_{[i]}, y_{[j]})$ for all values of P and it must satisfy the equation given below at infinity point [15].

$$y^2_{[j]}+c_1x_{[i]}\, y_{[j]}+c_3y_{[j]}=x^3_{[i]}+c_2x^2_{[i]}+c_4x_{[i]}+c_6$$

The curve w.r.t P for elliptical curve K is P(K), the points on P for all values P for various fields introduction in [14]. The ECC field is usually represented in form of complex which consists both real and rational numbers compared to finite curve field, in both fields uses the prime number for high security and more complexity in ECC systems depends on crack to ability of the curve is generally known as Discrete Logarithmic Problem (DLP) [16]. One of the famous algorithm in ECC for high security is ElGamal cryptography for both encryption and decryption discussed in [13, 16]. To exchange the key as public key, the Diffie and Hellman introduced by cryptography [20] in the year of 1976 later stage for less key size RSA has been invented [19]. IEEE 802.16 protocol is mainly for WiMAX protocol to transfer the data through wirelessly which is part of physical and control layer in OSI model to use in point to point communication and it uses the mesh mode topology. Other than these two layers, there are another types of layer for the association of security to the data and for authorization and authentication purpose is discussed in [23, 28]. For encoding of data, modulation of carrier signal and modulation of frequencies uses the physical layer than control layer. The main sub module for the security is MAC and it will act as convergence and controlling of data transfer from transmitter to receiver [24,25]. In ECC concept, the new methods for data encryption are Menezes Vanstone which is basically dividing the main module into smaller blocks like pipeline process and it contains the one character in terms of hexadecimal format. The each hexadecimal value has two digits to express the information as point [21].

II. METHODOLOGY

Many methodologies have been broke down from various area examine researchers and ventures to give the security to messages, computerized data, extraordinary characters and pictures [9]. The vital parameters for every one of these applications is key size, if the key length is bigger, higher the security [10]. These are numerous encryption and decoding calculations like BCH, hamming codes, piece codes like LDPC, RS codes and AES, out of which AES utilizes most extreme key length i.e. 256 bits and different calculations utilize just 8 bits key length. At that point a most essential contending framework that has developed and high security key age is Elliptic Curve Cryptography (ECC) since this framework opened a riches conceivable outcomes as far as high security [11]. In the present work, novel idea is proposed to build up the model framework basic and high security for the sorts of information's. In this work, ECC has been adjusted for the age of 256 distinctive keys to shape a 16x16 framework; each key size is 32 bits which incorporates two unique characters know by the sender and collector. This unique character joins x and y arranges appeared in condition (1).

$$\text{Key}_{\text{special characters}} = (x \,\&^{*}\, y) \qquad (1)$$

Where & is the special character of sender and * is the special character of receiverIn ECC cryptography framework, the novel worry with a confined type of elliptic bend that is characterized over a limited field (ffp). The imperative number is p called "mod p", it is gathering of elliptic gathering and p dependably s prime number and it is characterized as a condition (2).

$$(4G_1^3 + 27G_2^2) mod\ p \neq 0 \qquad (2)$$

andE_p represents the elliptic group mod p of coordinates (x,y) is the pair of nonnegative integer and less than p, it should satisfy the equation (3)

$$y^3 = (x^3 + G_1x + G_2) mod\ p \qquad (3)$$

The $E_p(G_1, G_2)$ group has many numbers of points including all special characters and infinity (Ω).

Generation of points on the curve

To fulfill the eq (2) and eq (3), G1=1 and G2=1 are picked. To frame 16x16 network, the aggregate number of focuses required are 256, for which p=463 is chosen, on the grounds that according to ECC control, the higher the p esteems progressively the security of the outlined framework [12, 21]. The p number esteems go from 1 to 463 and substitute the all numbers in eqn's. (3 and 4) on LHS and RHS sides. The condition of LHS is spoken to in eqn. (4) and RHS condition is spoken to in eqn. (5).

$$y_{coordinate} = y^2 mod\ p \qquad (4)$$
$$x_{coordinate} = (x^3 + G_1x + G_2) mod\ p \qquad (5)$$

The calculated result values of LHS and RHS are listed in Annexure-I. From the Annexure-I, the coordinated directions point (x, y) are recognized, for p=463 there are just 10 coordinated focuses and those coordinated are shown in red shading in Annexure-1. The one of the coordinated focuses is chosen as starting point, i.e. P= (70,86) and utilizing this underlying point, the following focuses like 2p,3p,4p,5p, … ..,256p are computed by utilizing point expansion (PA) and point multiplying (PD). The figured 256 focuses are recorded in the Table.1. The benefits of PA and PD are to lessen the quantity of math operations and scalar increase i.e kp where k is consistent shifts from 1 to 463. The conditions of PA and PD are given in eqn. (6) and eqn. (7).

Points	Points on the elliptic curve							
1-8	(70,86)	(270,328)	(226,429)	(104,86)	(294,324)	(73,287)	(179,19)	(390,302)
9-16	(182,394)	(299,334)	(82,271)	(304,401)	(223,82)	(292,1)	(268,134)	(373,216)
17-24	(8,153)	(321,232)	(283,100)	(256,280)	(258,161)	(122,32)	(68,226)	(235,354)
25-32	(102,36)	(132,197)	(392,383)	(244,241)	(95,384)	(137,59)	(438,394)	(34,294)
33-40	(78,166)	(139,377)	(137,336)	(449,340)	(8,410)	(90,109)	(324,409)	(14,150)
41-48	(437,135)	(334,59)	(237,10)	(263,414)	(246,289)	(430,45)	(374,200)	(8,273)
49-56	(228,286)	(253,407)	(296,269)	(428,80)	(236,222)	(339,6)	(217,315)	(304,391)
57-64	(157,412)	(432,204)	(251,274)	(15,11)	(24,103)	(442,13)	(112,327)	(126,378)
65-72	(306,337)	(73,53)	(441,291)	(355,406)	(87,33)	(178,11)	(73,53)	(110,452)
73-80	(16,84)	(424,261)	(253,73)	(162,144)	(328,293)	(247,16)	(276,402)	(13,93)
81-88	(452,275)	(358,123)	(166,56)	(417,225)	(117,365)	(175,19)	(225,44)	(433,96)
89-96	(29,279)	(157,380)	(330,137)	(206,158)	(29,451)	(10,80)	(258,173)	(139,52)
97-104	(126,102)	(97,237)	(67,144)	(53,64)	(284,209)	(203,108	(83,347)	(272,346)
105-112	(13,267)	(366,131)	(328,258)	(14,260)	(162,51)	(187,34)	(374,154)	(14,24)
113-120	(69,97)	(445,335)	(186,367)	(56,371)	(64,321)	(384,20)	(343,225)	(154,259)
121-128	(79,375)	(328,147)	(214,121)	(31,454)	(27,458)	(75,108)	(82,56)	(239,162)
129-136	(239,162)	(376,12)	(82,14)	(347,187)	(306,195)	(205,34)	(321,298)	(73,380)
137-144	(59,348)	(423,72)	(299,162)	(407,158)	(125,376)	(93,382)	(437,4)	(182,127)
145-152	(399,134)	(315,292)	(93,369)	(370,128)	(241,66)	(209,26)	(188,434)	(308,452)
153-160	(146,289)	(428,164)	(318,58)	(330,257)	(69,351)	(173,35)	(282,395)	(58,80)
161-168	(451,418)	(11,172)	(81,189)	(128,339)	(132,441)	(384,22)	(212,225)	(230,155)
169-176	(37,17)	(104,348)	(162,440)	(155,60)	(217,199)	(357,44)	(167,166)	(415,160)
177-184	(419,280)	(282,356)	(175,78)	(31,83)	(36,304)	(4,19)	(234,274)	(295,232)
185-192	(441,334)	(303,142)	(444,412)	(204,332)	(62,136)	(399,23)	(150,333)	(329,104)
193-200	(179,205)	(286,18)	(44,334)	(303,142)	(444,412)	(204,33)	(62,136)	(399,234)
201-208	(107,275)	(51,424)	(455,67)	(143,9)	(334,89)	(347,95)	(271,6)	(21,293)
209-216	(97,50)	(187,34)	(186,281)	(225,320)	(211,427)	(387,59)	(3,81)	(334,226)
217-224	(33,165)	(210,288)	(154,259)	(79,375)	(154,122)	(88,237)	(202,258)	(66,284)
225-232	(401,183)	(81,115)	(384,391)	(373,267)	(369,152)	(369,15)	(260,397)	(15,206)
233-240	(157,188)	(360,150)	(92,254)	(127,347)	(42,359)	(217,11)	(218,181)	(135,287)
241-248	(292,182)	(19,317)	(151,63)	(14,31)	(262,453)	(38,407)	(145,131)	(173,438)
249-256	(456,312)	(249,337)	(366,143)	(413,354)	(395,254)	(42,313)	(337,177)	(199,64)

Table.1. Generated 256 points using PA and PD which are on the ECC curve

Point addition

Let p=(x_1, y_1) and q=(x2, y_2), both p & q are belongs to ff_p then p+q=(x3, y_3)
Where

$$x_3 = \left[-x_1 - x_2 + \left(\frac{y_2-y_1}{x_2-x_1}\right)^2\right] mod\ p \qquad (6)$$

And

$$y_3 = \left[-y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3)\right]\ mod\ p \qquad (7)$$

Where $\left(\frac{y_2-y_1}{x_2-x_1}\right)$ is represented as λ and if λ is negative then the following special cases to be considered to satisfy the ECC basic condition,

(1) If the numerator is negative then the either of the following procedure can be used
   (i) Take modulo operation for the negative numerator value (or)
   (ii) Take inverse of denominator then use signed multiplication

(2) If denominator is negative then the either of the following procedure can be used
   (i) Take modulo operation for the denominator value (or)
   (ii) Take inverse of denominator then use signed multiplication

(3) If both are negative then the either of the following procedure can be used
   (i) Take modulo operation for the numerator and denominator values (or)
   (ii) Find the inverse of denominator and then multiply it with numerator

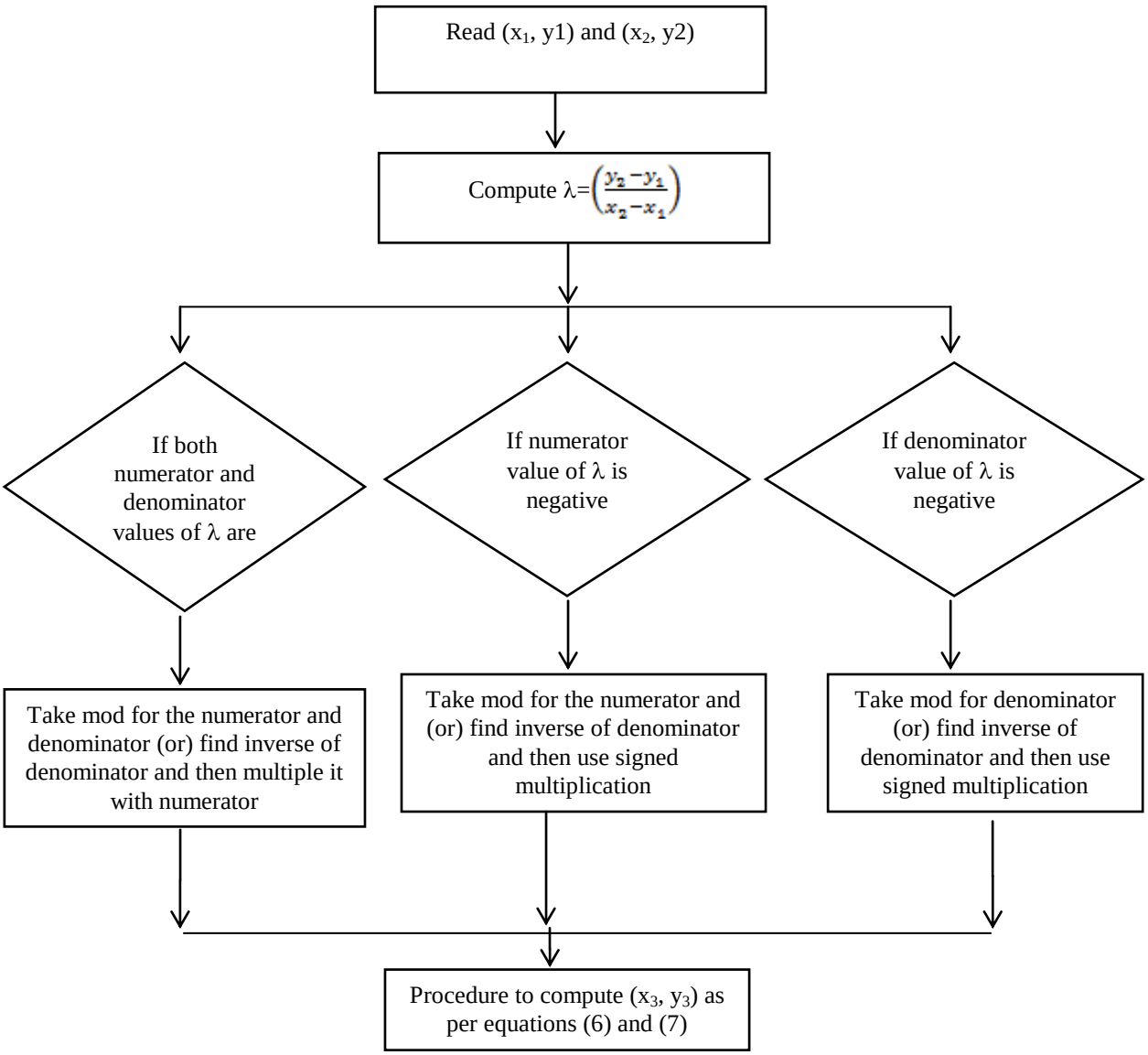

Fig.1 Flow chart for finding of sign in λ.

Point doubling (PD)

If input is single point then PD can be used to generate a doubling of the point, for example 2p=p+p, 4p= 2p+2p, 8p=4p+4p, etc. To perform PD on single point say p,2p,4p,……, so on, let take p=(x_1,y_1) then 2p=(x_3,y_3), where

$$x_3 = \left[-2x_1 + \frac{3x_1 - G1}{2y_1^2}\right] mod\ p \text{And}$$

$$y_3 = \left[-y_1 + \frac{3x_1 - G1}{2y_1^2}\right] mod\ p$$

By utilizing PA and PD, the 256 focuses are produced and same focuses are recorded Table.3. Furthermore, this Table is the 16x16 framework. Each point comprises of both x and y facilitates. To perform facilitate operation by advanced processors, the x and y arranges are joined into single an incentive by embedding's two exceptional characters between them. The sizes of each organize are 8-bit and size of unique character is 8 bit, along these lines the aggregate size of the fact of the matter is 32 bits as appeared in condition (8).

$Key_{special\ characters}$=(x &* y) =(70&*86) (8)

The parallel portrayal of 70 is 1000110, the double portrayal of 86 is 1010110, the twofold portrayal of and is 00100110 and the paired portrayal of * is 00101010 so the condition (8) can be compose $Key_{special\ characters}$=10001101010110001001100010101O. The 32 bits of twofold information is contribution to the encryption. After effectively age of 256 focuses utilizing PA and PD, every one of the focuses are amassed Look-Up-Table (LUT) and relying upon the 8 bit input information, 32 bit of LUT esteem will be chosen. The 32 bit LUT esteem is transmitted through correspondence subsystems like, Routers or Network Interface (NI). To decrease the power dissemination in NI before transmission of information through correspondence channel, the information will be encoded; the encoded yield information ought to guarantee the quantity of advances will be least. In the proposed work, three strategies are introduced to diminish the number changes, every strategy is propelled adaptation of past one as far as advances.

The primary techniques can lessen just 25% of advances, half of advances decrease in second strategy and 85% diminishment in third technique. These techniques are dissected and looked at regarding power dispersal decrease which is relative to number of changes.The power dissipation in the NI is given in equation (9)

$$p = [NIT_{0\,to\,1}(C_s + C_l) + T_c\,C_c]V_{dd}^2 f_{clock} \quad (9)$$

Where $NIT_{0\ to\ 1}$ is the aggregate number of changes in the transmission information, Cs is the substrate capacitance, Cc is the coupling capacitance Cl is the heap capacitance and f_{clock} is the info clock recurrence. The coupling capacitance Cc is real reason for control dissemination and advances are because of Cc can be any of one of the accompanying conditions

1. Advances can happens when one of the CMOS switch is condition state and the others are unaltered.
2. Changes can happens when one of the CMOS change, changes from low to high while the others makes progress from high to low.
3. At the point when both switch are at the same time switches
4. At the point when both switches are don't change the states

Consequently change in Cc is T_{Cc} is a weighted total of various states of coupling advances and it can be compose as appeared in condition (10)

$$T_{C_c} = W_1 T_1 + W_2 T_2 + W_3 T_3 + W_4 T_4 \quad (10)$$

Where T_1 , T_2 , T_3 and T_4 are the transitions for different condition, W_1 , W_2 , W_3 and W_4 are weights of their corresponding conditions and the following are the example of all four conditions

T_1: 00 11 or 01 10 T_2: 00 11 T_3: 00 11 01 10
10 01 11 00 11 00 00 11 01 10

T_4: 01 10
10 01

The number of transitions from 0 to 1for two consecutive flits is counted.

Novel Encoder using BTED:

Step 1: Read 32 bit of data from 16x16 matrix. Let X be the input data say X=10110011101011011011001111010110 1

Step 2: Perform right shift operation (T_y) on input 32 bit data

X=10110011101011011011001111010110 1

T_y=00101100111010110110110011101011

111111 1 11 1 1 11111 1 1 1

Step 3: Find the transitions between input data and shifted data.

The number of transitions in shifted data is 19 so after encoding the number of transitions should be less than 19 to say power has been reduced.

Step 4: Find type of inversion i.e whether half, full or No inversions using $T_y > \frac{W-1}{2}$, where W is size of the input data i.e 32 bit

$$T_y > \frac{32-1}{2} = 15.5$$

If $T_y > \frac{W-1}{2}$ then odd invert is 10, even invert is 01, full invert is 11 and 00 is the No inversion

Step 5: Perform XOR operation between input data, even and odd invert to get encoded data (Z) is shown below

Z[0]=X[0]XOR event invert =1XOR 1=0
Z[1]=X[1]XOR odd invert =0XOR 1=1
Z[2]=X[2]XOR event invert =1XOR 1=0
Z[3]=X[3]XOR odd invert =1XOR 1=0
Z[4]=X[4]XOR odd invert =0XOR 1=1
Z[5]=X[5]XOR odd invert =1XOR 1=0
Z[6]=X[6]XOR odd invert =0XOR 1=1
Z[7]=X[7]XOR odd invert =1XOR 1=0
Z[8]=X[8]XOR odd invert =1XOR 1=0
Z[9]=X[9]XOR odd invert =1XOR 1=0
Z[10]=X[10]XOR odd invert =0XOR 1=1
Z[11]=X[11]XOR odd invert =0XOR 1=1
Z[12]=X[12]XOR odd invert =1XOR 1=0
Z[13]=X[13]XOR odd invert =1XOR 1=0
Z[14]=X[14]XOR odd invert =0XOR 1=1
Z[15]=X[15]XOR odd invert =1XOR 1=0
Z[16]=X[16]XOR odd invert =1XOR 1=0
Z[17]=X[17]XOR odd invert =0XOR 1=1
Z[18]=X[18]XOR odd invert =1XOR 1=0
Z[19]=X[19]XOR odd invert =1XOR 1=0
Z[20]=X[20]XOR odd invert =0XOR 1=1
Z[21]=X[21]XOR odd invert =1XOR 1=0
Z[22]=X[22]XOR odd invert =0XOR 1=1
Z[23]=X[23]XOR odd invert =1XOR 1=0
Z[24]=X[24]XOR odd invert =1XOR 1=0
Z[25]=X[25]XOR odd invert =1XOR 1=0
Z[26]=X[26]XOR odd invert =0XOR 1=1
Z[27]=X[27]XOR odd invert =0XOR 1=1
Z[28]=X[28]XOR odd invert =1XOR 1=1
Z[29]=X[29]XOR odd invert =1XOR 1=0
Z[30]=X[30]XOR odd invert =0XOR 1=1
Z[31]=X[31]XOR odd invert =1XOR 1=0

Record the result bits from most significant bit (MSB) to least significant bit (LSB) to get encoded output i.e 01011100010100100100110001010010

Step 6: Store the encoded data in memory for decoder operation

Step 7: Perform step1 to step 6 for next consecutive input data

Novel Decoder using BTED:

Step 1: Read 32 bit of data from encoder memory output. Let Z be the input data say Z=01011100010100100100110001010 1

Step 2: Perform right shift operation (T_y) on input 32 bit data

Z=01011100010100100100110001010 1
T_y=00010111000101001001001100010100

---

1 1 11 1 11 11 11111 11

Step 3: Find the transitions between input data and shifted data

The number of transitions in shifted data is 17 so after encoding the number of transitions should be less than 19 to say power has been reduced.

Step 4: Find type of inversion i.e whether half, full or No inversions using $T_y > \frac{W-1}{2}$, where W is size of the input data i.e 32 bit

$$T_y > \frac{32-1}{2} = 15.5$$

If $T_y > \frac{W-1}{2}$ then half invert is 10, full invert is 01 and 00 is the No inversion

Step 5: Perform XOR operation between encoded data, full and half invert to get decoded data (Z) is shown below

X[0]=Z[0]⊕full invert =0⊕ 1=1
X[1]=Z [1]⊕full invert⊕half invert =1⊕ 1⊕0=0
X[2]=Z[2]⊕full invert =0⊕ 1=1
X[3]=Z[3]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[4]=Z[4]⊕full invert =1⊕ 1=0
X[5]=Z[5]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[6]=Z[6]⊕full invert =1⊕ 1=0
X[7]=Z[7]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[8]=Z[8]⊕full invert =0⊕ 1=1
X[9]=Z[9]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[10]=Z[10]⊕full invert =1⊕ 1=0
X[11]=Z[11]⊕full invert⊕half invert =1⊕ 1⊕0=0
X[12]=Z[12]⊕full invert =0⊕ 1=1
X[13]=Z[13]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[14]=Z[14]⊕full invert =1⊕ 1=0
X[15]=Z[15]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[16]=Z[16]⊕full invert =0⊕ 1=1
X[17]=Z[17]⊕full invert⊕half invert =1⊕ 1⊕0=0
X[18]=Z[18]⊕full invert =0⊕ 1=1
X[19]=Z[19]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[20]=Z[20]⊕full invert =1⊕ 1=0
X[21]=Z[21]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[22]=Z[22]⊕full invert =1⊕ 1=0
X[23]=Z[23]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[24]=Z[24]⊕full invert =0⊕ 1=1
X[25]=Z[25]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[26]=Z[26]⊕full invert =1⊕ 1=0
X[27]=Z[27]⊕full invert⊕half invert =1⊕ 1⊕0=0
X[28]=Z[28]⊕full invert =1⊕ 1=0
X[29]=Z[29]⊕full invert⊕half invert =0⊕ 1⊕0=1
X[30]=Z[30]⊕full invert =1⊕ 1=0
X[31]=Z[31]⊕full invert⊕half invert =0⊕ 1⊕0=1

III. RESULTS AND DISCUSSION

The proposed BEDT system is designed for three different circuits and each is an extended version of the previous circuit. When mux is "00", scheme I, "01" for scheme II and "10" for scheme III will be selected.

Assume that if the 32-bit date is 10101011101010111010101110101011, total number of the transitions on the assumed date is 24, and after encoding, the number of transitions is reduced to 12, as represented in Figure 2. So that the rate of traffic reduction in scheme I is 50%, as shown in the example

- Number of transitions in the input data = 24
- Coded output = 1010101110101011
- Number of transitions in coded output = 12
- Output of scheme 1 = 10101011101010111010101110101011

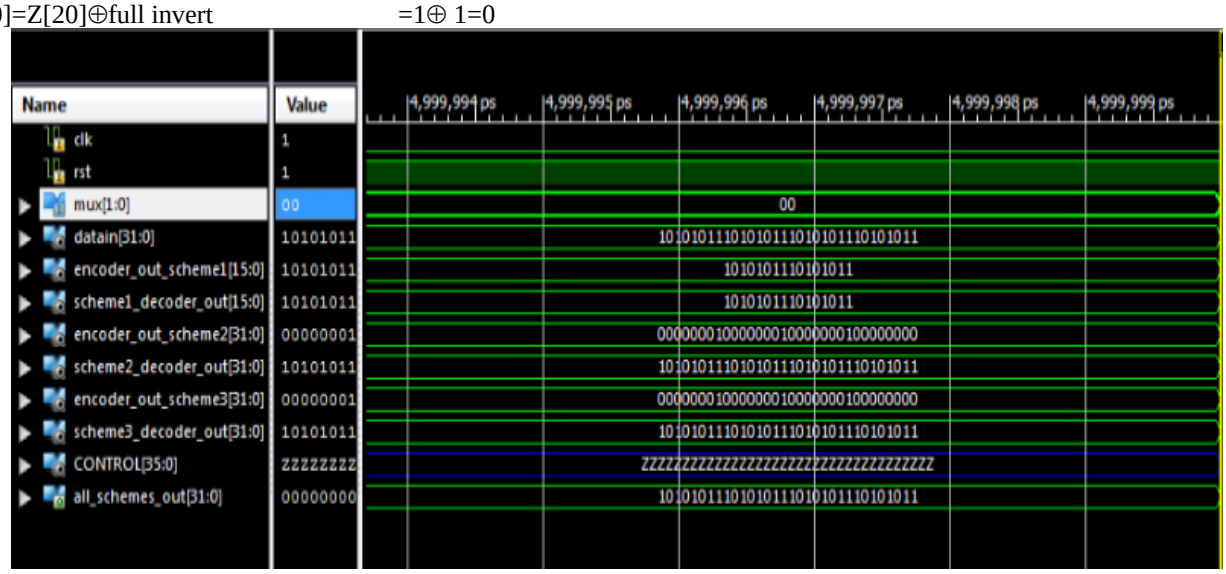

Fig.2. Simulation resutls of Scheme-I for both encryption and decryption when mux is "00"

Scheme II is better than Scheme I since number of transitions is up to 6, therefore, percentage deduction in number of transitions is 75%. The following is an example of Scheme II and its input and output data after encryption and decryption are shown in Figure 3.

- Mux = 01
- Data in = 10101011101010111010101110101011
- Number of transitions in the input data = 24
- Coded output = 10000000100000001000000100000001
- Number of transitions in coded output = 8
- Output of scheme 2 = 10101011101010111010101110101011

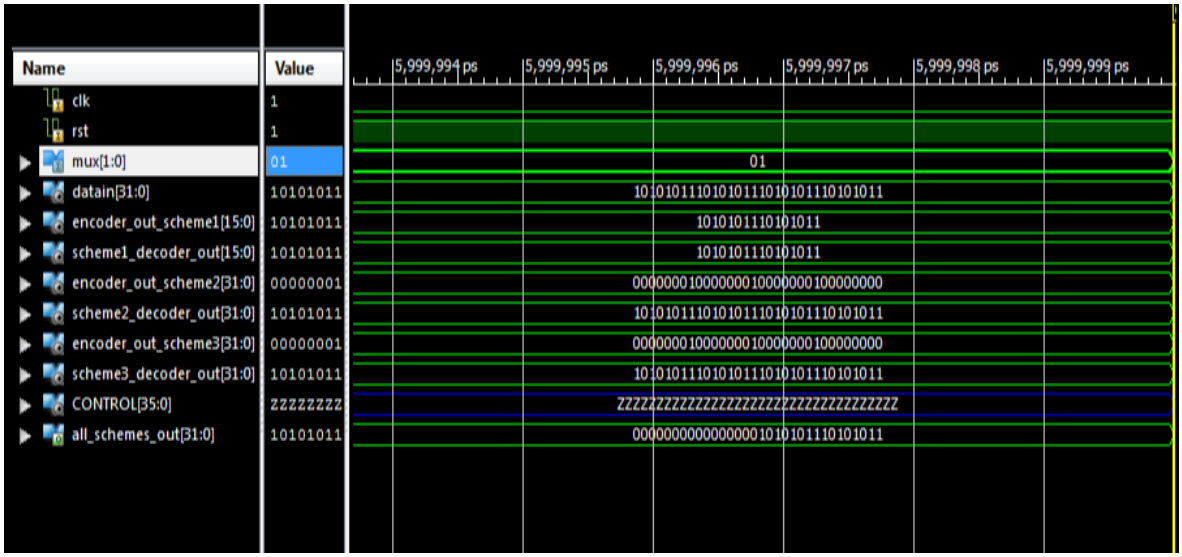

Fig.3. Simulation resutls of Scheme-II for both encryption and decryption when mux is "10"

In Scheme III, the number of transitions is only 6; therefore, the conversion rate reduction rate is almost 85%, so Scheme-III is the best cryptographic technique for the reduction of safety and power. The following example shows Scheme III together with encryption and decryption scheme.

- Mux = 10
- Data in = 10101011101010111010101110101011
- Number of transitions in the input data = 24
- Coded output = 00000001000000010000000010000000
- Number of transitions in coded output = 6
- Output scheme 3 = 10101011101010111010101110101011

Conclusion and discussion

The novel procedure for proposed cryptography is more viable as far as speed, security, power and intricacy since the framework utilizes just XOR and straightforward scientific operation which are less utilization equipment assets. The bit progress operation for both encoder and decoder are to diminish the power for the most part in organize applications like NoC and SoC chips which are utilized as a part of wired and remote correspondence for quick exchanging activity between any two information transmission and gathering. The ETED for encoder and decoder are predominantly to decrease the power utilization and ETED are joined with ECC for age of exceedingly secret keys to scramble and unscramble the ongoing information through either wired or remote system channels. The proposed configuration is tried in Matlab 2014a and approved the outcomes on Field programmable Gate Array (FPGA) equipment leading group of Virtex-5 (XC5VLX50T+1136) with Zigbee convention.

Acknowledgements

The Author is very much thankful to University Grant Commission (UGC) Govt. of .India for supporting and Funding the research through Minor Research Project– Application Number MRP-6958/16(SERO/UGC).

REFERENCES

1. Arunkumar, "A Comparative Study of Public Key Cryptosystem based on ECC and RSA" International Journal on Computer Science and Engineering (IJCSE), International University, Faridabad, India, 2011.
2. O.SRINIVASA RAO,"EFFICIENT MAPPING METHODS FOR ELLIPTIC CURVE CRYPTOSYSTEMS", International Journal of Engineering Science and Technology, Andhra Pradesh, India,2010.
3. Riaz Naseer "Parallel Double Error Correcting Code Design to Mitigate Multi-Bit Upsets in SRAMs," IEEE. Abbreviation 978-1-4244-2361-3/08/$25.00 ©2008
4. Juan Antonio Maestro, "Soft error tolerant Content Addressable Memories (CAMs) using error detection code and duplication," Elsevier B.V @2013.
5. Gustavo Neuberger "An Automatic Technique for Optimizing Reed – Solomon Codes to Improve Fault Tolerance in Memories," IEEE Design & Test of Computers, Copublished by the IEEE CS and the IEEE CASS @2005 .
6. SanghyeonBaeg, "Analysis of a Multiple Cell Upset Failure Model for Memories"
7. Sandeep M D, "An Approach to Reduce Number of Redundant Bits used To Overcome Cell Upsets in Memory using Decimal Matrix Code," Proc. Of Int. Conf. on Recent Trends in Signal Processing, Image Processing and VLSI, ICrtSIV, ACEEE,2014
8. Costas Argyrides, ,"Area Reliability Trade – Off in Improved Reed Muller Coding," SAMOS 2008, LNCS 5114, pp. 116-125, 2008 Springer – Verlag Berlin Heidelberg 2008.
9. Bertozzi,. "Error control schemes for on-chip communication links:the energy-reliability tradeoff". IEEE Trans. on DAC 24(6) (June 2005).
10. Rossi, "Error correcting strategy for high speed and density reliable flash memories". IEEE J. Electronic Testing, Theory and applications 19(5), 511–521 (2003).
11. Argyrides, "Improved Decoding Algorithm for High Reliable Reed Muller Coding"20th IEEE International System On Chip Conference (SOCC 2007).
12. F.Amounas, "Fast mapping method based on matrix approach for elliptic curve cryptography", International journal of information and network, Vol.1, No.2.
13. Victor S, "Use of elliptic curves in cryptography" In: Proceeding of the Advances in Cryptology-Crypto'85, LNCS, Springer-Verlag, pp. 417-426, 1985.
14. Neal Koblitz, " The state of elliptic curve cryptography" Design, Codes and Cryptography, Vol 19, Issue 2-3, pp.173-193, 2000.
15. DarelHankerson, "Guide to Elliptic Curve Cryptography", Springer-Verlag, 2004

16. M. Kurt "Encryption with Changing Least Significant Bit on Menezes Vanstone Elliptic Curve Cryptosystem ", pp. 1-3, Conference paper MAY 2014.
17. Fatima Amounas, "An application of discrete algorithms in asymmetric cryptography", International Mathematical Forum 6 (49), pp. 2409-2418, 2011.
18. Prashant Sharma,"Modified Elgamal Cryptosystem Algorithm (MECA)", International Conference on Computer & Communication Technology (ICCCT)-2011, pp 439-443.
19. Swadeep Singh, "Comparision of Cryptograpic Algorithms ECC and RSA", International Journal of Computer Science and Communication Engineering (IJCSC), Special issue on "Recent Advances in Engineering & Technology" NCRAET2013.
20. P. K. Shau, "An Implementation of Elliptic Curve Cryptography", International Journal of Engineering Research and Technology (IJERT) ISNN: 2278-0181, Vol 2 Issue 1, January 2013.
21. M. Kurt, "A New Modified Cryptosystem Based on Menezes Vanstone Elliptic Curve Cryptography Algorithm that Uses Characters' Hexadecimal Values", TAEECE 2013, Konya, Turkey, 2013.
22. T. Wollinger, "Security on FPGAs: State-ofthe-art implementations and attacks," IEEE Trans.EmbeddedComput. Syst., vol. 3, no. 3, pp. 534–574, Aug. 2004.
23. Do-Hyeon Choi, "ECC-based Mobile WIMAX Initial Network Entry with Improved Security" International Journal of Advanced Computer Technology (IJACT) : , Vol. 5, No. 13, pp. 505 ~ 517, 2013
24. " Air interface for fixed broadband wireless access systems", IEEE Computer Society and IEEE Microwave Theory and Techniques Society, 802.16-2004,Oct. 2004.
25. M. IndraSena Reddy "Key Distillation process on Quantum cryptography protocals in Network Security", International journal of Advanced Research computer science and Software Engineering, Vol.2, Issue 6**,** 2012.
26. K Subba Reddy "A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography", International Journal of Computer Applications. ISSN (0975 – 8887) Volume 67– No.10, April 2013.
27. K Subba Reddy "Secured Data Transmission using Wavelet based Steganography and Cryptography", International Journal of Computers & Technology. ISSN 2277-3061 Volume 6– No.1, April 2013.
28. M Purusotham Reddy "Host Based Information Gathering Honeypots for Network Security", International Journal of computational Engineering & research. ISSN 2250-3005 Volume 2– Issue No.2, April 2012.
29. M. IndraSena Reddy, "Wireless Application Protocol for Potential Threats to Mobile Agent Network Security", Journal of Electronic science and Technology**,** VOL.10**,** NO.3, September 2012, Digital Object Identifier: 10.3969/j.issn.1674-862X.2012.03.005

AUTHORS PROFILE

M. Indrasena Reddy is working as Assistant Professor in the Department of Computer Science & Engineering. He graduated in 2009, Masters in 2011and pursuing Ph.D. degree in computer science & engineering from Jawaharlal Nehru Technological University, Anantapuramu. Recipient of Minor Research Project for the Financial Year 2014-2015 with grant of Rs 3,10,000/ by UGC, New Delhi. He has published 13 papers in Various International Conferences and journals. He is currently doing research on network security with the Department of Computer Science & Engineering, RGM College of Engineering and Technology. His research interests include information security and computer networks.

Mr Dr.A.P.Siva Kumar, did his B.Tech from JNTUH, M.Tech from JNTUA, Ph.D from JNTUA in area of "Information Retrieval and Cross Lingual Intelligent Systems"in Year 2011. Recipient of Carrer Award for Young Teachers (CAYT) for the Financial Year 2013-14 with grant of Rs 1,50,000/ AICTE, New Delhi.He currently teaches in the Department of Computer Science and Engineering. His subjects of interest include Data Analytics, Natural Language Processing, Software Project and Process Management, Software by Testing Methodologies, Information Retrieval ,Computer Organization, Operating systems, etc.,Developed Examination Management Software "JEMS" JNTUA Examination Management System (EMS) which automates various tasks and procedures associated with the pre-examination and the post-examination phases associated with the Examination branch of an Autonomous College.Currently the Software is in live at JNTUCE Pulivendula and Audisankara College,Gudur. Master Trainer of Associate Analytics Trained by Nasscom in association with APSSDC.