GLOBAL ACADEMIC RESEARCH INSTITUTE

COLOMBO, SRI LANKA

GARI International Journal of Multidisciplinary Research

ISSN 2659-2193

Volume: 04 | Issue: 03

On 15th June 2018

http://www.research.lk

Author: Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R

VTU-Research Centre, India

GARI Publisher | Networking | Volume: 04 | Issue: 03

Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)

ISSN 2659-2193 | Edit: GARI Editorial Team

Received: 18.05.2018 | Publish: 15.06.2018

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

IMPLEMENTATION OF DOUBLE ENCRYPTION USING ELGAMAL AND KNAPSACK ALGORITHM ON FPGA FOR NODES IN WIRELESS SENSOR NETWORKS

[1]Leelavathi G, [2]Dr.Shaila K, [3]Dr.Venugopal K R
[1,2]VTU-Research Centre, [3]University Visvesvaraya College of Engineering, India.
[1]nisargamodini@gmail.com

ABSTRACT

The primary objective of this proposed work is to implement elliptical curve cryptography with matrix mapping techniques and knapsack algorithm for information encryption and decryption in nodes of Wireless Sensor Networks. In this paper through mapping method there is complication to guess the phrases as it does not show any regularity and knapsack algorithm avoids brute drive attack by growing confusions. The modules are integrated to perform matrix mapping, Knapsack encryption, knapsack decryption and de mapping. Verilog language is used for coding and simulation is completing on Xilinx ISE 13.4 and Spartan 6, Kintex 5 and Artix 7 FPGAs are used as the hardware. The complete crypto process is executed with frequency of 503.702MHz. No Maximum combinational path delay is found in the implementation of modules. In comparison with previous works the area utilization in this work is very less, thus satisfying the resource constraints' of wireless sensor nodes.

Keywords: Elliptic Curve Cryptography, FPGA, Knapsack Algorithm, Matrix Mapping, Wireless Sensor Networks.

INTRODUCTION

The problem of securing Wireless Sensor Networks (WSNs) has been one of the challenging research areas in the field of network security. In Embedded system market, WSNs applications have greater share with promising future. WSNs are deployed in many real-world applications, including Ambient Intelligence and Ubiquitous Computing. Owing to scarcity of energy, unsecure channel and intensive mathematical operations of asymmetric cryptographic primitives, it is difficult to realize secure WSNs. Due to these exclusive challenges, security of WSNs become a very important topic in the research area. Many mechanisms are explored to provide security for WSNs [1] [2] [3].

Security of the information is significant issue; cryptography takes an important place in exchanging of information by secure way. There have been numerous efforts to secure applications efficiently, engaging a various choice of security techniques. The resource constrained nodes are subjected to issues with, latency, power consumption, and processor usage and memory requirements. There is continuously a resource consumption trade-off exists when flexibility in the levels of security is invoked for different applications [4]- [11].

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

Consequently, a fundamental of effective cryptography scheme is designing system with less key size. Size of the parameter is the chief advantage over RSA, because ECC delivers high computational protection than RSA in small number of bits only.

Static and dynamic mapping are two methods in Mapping of character into points on the curve. Static mapping accomplishes, for the same x-y coordinates it maps the same characters of the different words, the points generated is also same when encrypted. With the use of trial and error process third person interpret the message in this technique. With this technique secret of message transformation is low.

The dynamic mapping performs, for the different points of curve maps the different characters. This methodology is composite for a hacker to find out which point is taken for which character. However mapping process making use of matrix process in this work ensures the security for the data. Due to the fact this process avoids the regularity within the resulting encrypted textual content. Therefore this method strengthens the cryptosystems and provides better efficiency.

Comparison of knapsack algorithm and RSA algorithm exhibits that, knapsack algorithm is improved because it is highly sophisticated and it is having high complexity. This algorithm diminishes brute force attack from a hacker by introducing confusions.

The advantages of using Reconfigurable Hardware FPGA for security algorithm implementations are Algorithm agility, Algorithm upload, Architecture efficiency, Resource efficiency, Algorithm modification, Throughput, Cost efficiency. Public Key Cryptography algorithms are the most promising schemes with respect to energy and time consumption, which makes it very suitable for data encryption in WSN. Conventional methods are measured to be too expensive for computational implementation in WSNs. To address this problem, there has been a lot of research into employing Public key infrastructures for WSNs. Given the deficiency of the resources for securing WSNs, attention was placed on the asymmetric key algorithms.

LITERATURE SURVEY

A key pre-distribution scheme for WSNs described in Shaila et al., [7]. Roy et al., [8] demonstrates appropriate scheduling for performing point addition and doubling in a pipelined data path of the ECSMA. Houssain et al., [9] delivers study of Elliptic Curve Cryptography (ECC) and hardware implementations with normal basis representation over GF (2m) in WSN. Rahuman et al., [10][11] offer Lopez-Dahab Elliptic Curve Point Multiplication algorithm. Hassan et al., [12-15] explore hardware/software co-design technique to understand a scalable Elliptic Curve Cryptography (ECC) processor.

Extreme safety of the Encrypted message is offered by a rapid mapping procedure i.e. matrix mapping. Encrypt and decrypt operation most effectively takes place on the curve but not using message in ECC. The points on elliptical

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

curve are mapped by the character and by using Elgamal encryption algorithm perform encryption and decryption operation. Geetha et. al., [15] takes up only Elgamal encryption on FPGA.

In the finite field GF (p) alphabetic message is transformed into points on elliptical curve to perform encryption and decryption making use of knapsack algorithm. This method increases the security by avoiding the brute force attack by developing confusions to the third person [16] and the implementation is not carried out on FPGA.

Table 1.Comparison work previous works with proposed work

Refer-ence No.	Algorithm/ Protocol/ Techniques	Advantages	Disadvantages	Device used FPGA
[15]	Matrix based mapping	Guarantee the confidentiality of messages hence providing better performance	Consumes more memory , power and less speed	Not Implemented FPGA
[21] [22]	An ECC protocol Based on Matrices	Less key size Bandwidth saving	Consumes more memory , power and less speed	Not Implemented FPGA
[23]	Matrix Based Elliptic Curve Cryptography Protocol	Enhances the security of ECC with multi fold encryption.	Consumes more memory , power and less speed	Not Implemented FPGA
[26]	ECC using Mealy Machine and Fibonacci Q-Matrix	Saves computation time and reduces power requirements	Consumes more memory and less speed	Not Implemented FPGA
[27]	ECC Cipher Processor Based On Knapsack Algorithm	Enhances the security of ECC with multi fold encryption	The maximum data size considered is 32 bit for analysis of speed and area	VIRTEX-2 SPARTAN-3E

In [1] it is defined about how the ECC is better than RSA in security of the data. Relating to RSA, key enchantment of ECC is, in small number of bit also offers same level of protection, it decreases processing complexity. The point operations are appreciated in performing encryption and decryption operations [17]. Guarantee the confidentiality of the messages can be achieved by using the matrix mapping method. Strength of the cryptosystem is increased by this mapping system [18][19]. ECC in cellular Wi-Fi and other applications is an important public key cryptography [20].

PROBLEM FORMULATION

Today many of the ECC systems are prepared. All are prefer only the system that should consume less power. Many of ECC systems designed with microprocessor having there is no compatibility with the instruction set and data path of the microprocessor and the finite field of the ECC system. Our goal is to design the system that should consume less power, and minimum area and less in memory usage.

Static mapping performs, for the same x-y coordinates it maps the same characters of the different words, for these points generated is also same when encrypted. The dynamic mapping performs, for the different points of curve maps the different characters. This methodology is complex for a hacker to find out which point is taken for which character. This system avoids the regularity within the resultant encrypted message, strengthens the crypto system and offers better performance. Comparing with RSA, ECC has an advantages considering that it supplies equal degree of security even for a small key dimension. .

CONTRIBUTION

Utilization of shorter key length in ECC is highly suitable for the wireless sensor node by consuming less power, minimum area and minimum bandwidth. Because of its hardware realization and software efficiency ECC is more efficient than RSA. In this work, a matrix mapping methodology and knapsack algorithm is implemented. In matrix mapping procedure transfer of all alphabetic character into points on elliptic curve is defined. Encryption and decryption of

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

mapping points is employed through knapsack algorithm. In this proposed work mapping method there is complicated to guess the phrases through it does no longer show any regularity and knapsack algorithm avoids brute drive attack by growing confusions. The language used to code these modules is Verilog. The modules are integrated to receive matrix mapping, Knapsack encryption, knapsack decryption and de mapping.

ELLIPTIC CURVE CRYPTOGR APHY

Elliptic Curve Cryptography (ECC) is a public-key cryptosystem that functions over points on an elliptic curve [20][21]. ECC operate directly on large integers. ECC is more efficient than other recognized public-key algorithms, due to its Elliptic Curve Discrete Logarithmic Problem (ECDLP). Equation (2) denotes to the general form of elliptic curve in Prime field GF (p). An elliptic curve group over real numbers contains the points on the equivalent elliptic curve, with O called the point at infinity.

$4m^3+27b^2 \bmod p \neq 0$ (1)

$y^2=x^3+ax+b \bmod p$ (2)

Scalar point multiplication is the primary operation in ECC, in cryptographic terms, that is performed through a combination of point additions and point doublings.

Scalar point multiplication computes the Point Q(x, y):

$$Q(x, y)=k*P(x,y) \quad (3)$$

Where a point *P(x, y),* an affine co-ordinate is multiplied by an integer k, which results in another point on the curve, *Q(x,y).* From ECDLP, given *P(x, y)* and *Q(x, y)* = k* *P(x, y)*, it is difficult to find *k*. A base point, *G(x, y)* generator point, is fixed for each curve. The random large integer, *k* acts as a private key; while multiplying *k* by the base point, *G(x, y)* results in corresponding public key. The best recognized technique for solving this problem is computationally infeasible for large values of k and the running time is completely exponential, in comparison with RSA or DSA, which have sub-exponential resolving speeds.

ECC POINT OPERATIONS

Point Inverse

If P = (x, y) Є E (Fp), then (x, y) + (x, – y) = ∞. The point (x, – y) Є E (Fp) and is called the inverse of J.

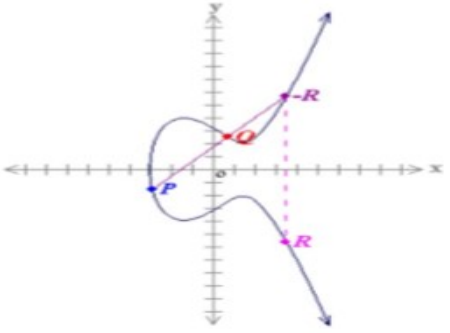
Given a point P(x1, y1) on an elliptic curve, -P(x1, y1) represents its inverse. The inverse of a given point can be computed using Equation 4.

$$-P(x1, y1)=P(x1, p- y1) \quad (4)$$

Point Addition

The Addition operator is defined over E (Fp) and it can be seen that E (Fp) forms an abelian group under addition. The addition operation in E (Fp) is specified by Equation (5)

$P + \infty = \infty + P = P$, P Є E (Fp) (5)



Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

Fig 1. The addition of two points.

If P = (x1, y1) Є E (Fp) and K = (x2, y2) Є E (Fp) and P ≠ Q, then R= P + Q = (x3, y3) Є E (Fp). Given two points on an elliptic curve, P (x1, y1) and Q(x2, y2), then the addition of those points results in L(x3, y3) which lies on the same curve as shown in Figure 1. It is figured using Equation 6, Equation 7 and Equation 8 as given in [4] and [5].

$$\lambda = (y2-y1)/(x2-x1) \quad (6)$$

$$x3 = \lambda^2 - x1 - x \quad (7)$$

$$y3 = \lambda(x1-x3) - y1 \quad (8)$$

Point Doubling

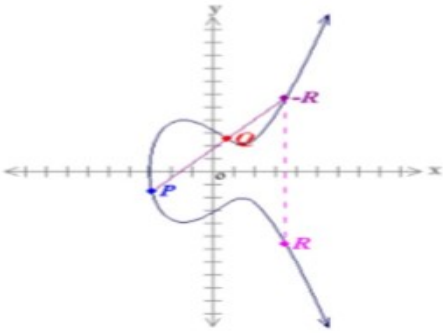


Fig.2 Doubling of a point

If P = (x1, y1) Є E (Fp), then R = 2 P = (x3, y3) Є E (Fp). Let J(x1, y1) be a point on the elliptic curve, then point doubling yields L(x3, y3) which lies on that curve as shown in Figure 2. It is computed using Equation 9, Equation 10 and Equation 11 as given in [4] and [5].

$$\lambda = (3x1^2 + a) / (2y1) \quad (9)$$

$$x3 = \lambda^2 - 2x1 \quad (10)$$

$$y3 = \lambda(x1-x3) - y1 \quad (11)$$

Scalar Multiplication

Given a point P(x1, y1) on the curve, to find k* P(x1, y1), where k is any integer, it needs repeated computations of point additions and point doublings. The reason for choosing prime fields is that distinct additive and multiplicative inverses exist for each number i.e. 0 to (P1) in the field of the prime number P.

In this proposed work, the operations point addition, point inverse, point subtraction, scalar multiplication are carried out on the points received from an elliptic curve equation (2) given in table 1.

ENCRYPTION AND DECRYPTION PROCESS

Figure 3 shows the Encryption block diagram which consists of three essential blocks, specifically point generation, matrix based mapping and knapsack encryption. While transmitting the information, both sender and receiver agree upon few conditions. Input is an undeniable text that can be converted into binary information. In that, undeniable textual content each and every letter is mapped as points on elliptical curve. This points are generatedd by using the chosen equation, this process is called as points generation. After the points are generated, in preliminary mapping points are mapped to alphabets. In matrix based mapping, storing all generated points into matrix form. Selecting one non singular matrix, multiply matrix points utilizing point addition and doubling approaches. Encyption process includes two methods i.e, ECC encryption and knapsack process. Knapsack process uses the

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

knapsack vector to encrypt the ECC encrypted data resulting in binary representation of cipher textual content[15][16].

Figure 4 suggests the decryption block diagram. Decryption Block Diagram consists of three major blocks, namely knapsack decryption block, matrix situated de mapping block, inverse of point generation block, Encrypted cipher textual content can be decrypted through using knapsack decryption algorithm. It involves two steps one is restoration of bit pattern from the encrypted text by way of utilizing inverse knapsack method and an additional decrypted way of ECC decryption procedure. Computing an inverse of non-singular matrix, multiplying decrypted data points matrix, by making use of point addition and doubling elliptic curve generated points are obtained. Using inverse of point generation, change the points on elliptic curve to text. Then output will be the textual content [17][18][19].

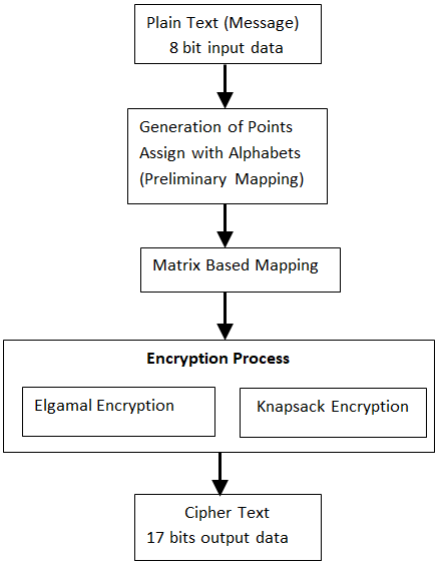


Fig 3. Flowchart of Encryption Process

At the beginning mapping and De mapping can be completed through using Matrix mapping methodology. Encryption and Decryption is applied utilizing Knapsack algorithm. Scalar multiplication is a main operation in ECC. All the modules are coded making use of Verilog language and simulation is completed on Xilinx ISE 13.2 and Spartan 6 , Kintex 5 and Artix 7 FPGA s are used as the hardware.

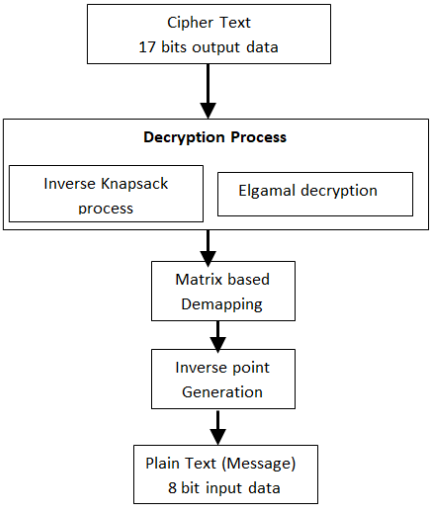


Fig 4. Flowchart of Decryption Process

ELLIPTIC CURVE POINT GEBERATION

In this proposed design the equation (2) of the elliptic curve is considered to generate the points on the curve. With this equation for simplicity, ‘a’ value is ‘1’; b value is ‘13’ and prime number p is ‘31’. All the operation takes place in the prime field and 34 points are generated. All this points are repeated after 34 points because these points are cyclic. Every generated point in a curve is having its inverse. First 26 points in a curve is

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

considered as 26 alphabets and remaining points are considered as numbers are special characters.

In point generation module instead of ASCII value, input is text data and output is the *x* and *y* mapping points on elliptic curve. For Example *"99"* is the ASCII value of the character 'c' whose mapping points on elliptic curve is *p(23,19),* where *x=23, y=19*. This type of mapping is called preliminary mapping. This preliminary mapping output points is input to the matrix based mapping. Figure 5 is the point generation RTL schematic and Figure 6 the point generation simulation result. Generated points are shown in table 1.

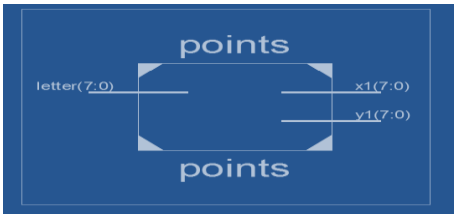


Fig 5. Generation of Points

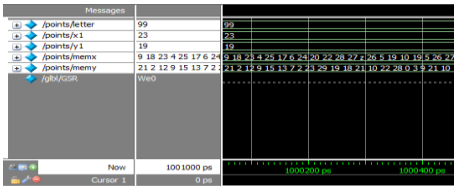


Fig 6. Timing Waveform of Elliptic Curve Points

P=(9,10)=A	7P=(6,24)=G	13P=(27,10)=M	19P=(5,22)=S	25P=(16,23)=Y	31P=(23,12)=%
2P=(18,29)=B	8P=(24,29)=H	14P=(26,21)=N	20P=(26,10)=T	26P=(24,2)=Z	32P=(18,2)=*
3P=(23,19)=C	9P=(16,8)=I	15P=(5,9)=O	21P=(27,21)=U	27P=(6,7)=' '	33P=(9,21)=∞
4P=(4,22)=D	10P=(20,2)=J	16P=(19,3)=P	22P=(28,18)=V	28P=(17,13)=!	--
5P=(25,16)=E	11P=(22,22)=K	17P=(10,0)=Q	23P=(22,9)=W	29P=(25,15)=@	--
6P=(17,18)=F	12P=(28,13)=L	18P=(19,28)=R	24P=(20,29)=X	30P=(4,9)=#	--

Table 2. Generated points of Elliptic curve

MATRIX MAPPING AND DE MAPPING METHOD

Both the sender and receiver agree upon few unique interactions between them that includes the elliptic curve equation, (*G (Fp)*) Set of elliptic curve points, (*P(x, y)*) Base (Generator) point of the elliptic curve, (*A*) Alphabets and special characters set, (*T*) Mapping points set, (*X* and X^{-1}) Non-singular matrix and its Inverse with only integer values, (*k*) Private key of Receiver, (*g*) Secret key of Sender. If A (sender) wishes to transmit a message *"CRYPTOGRAPHY"* to B (receiver). The generator point *P = (9, 10),* with *a = 1*, and *b = 13*. Then, representing the above message into a stream of points as follows: *{(23, 19), (19, 28), (16, 23), (19, 3), (26, 10), (5, 9), (6, 24), (19, 28), (9, 10), (19, 3), (24, 29), (16, 23)}*.

Matrix mapping method is the conversion of generated points in to another set of points in the elliptical curve. This is nothing but multiplication of generated points and non-singular matrix.

After generating, the points, using matrix based mapping approach these points are further mapped to gain high security. The matrix mapping module has 12 inputs and 12 outputs. Inputs to these matrix mapping points are *(23,19),(19,28), (16,23), (19,3), (26,10), (5,9), (6,24),(19,28),(9,10),(19,3),(24,29),(16,23)*. The output points getting from these matrix mapping module are *(22,4), (16,18), (9,4) ,(2,25) ,(15,24), (29,2) ,(12,24) , (5,27) ,(7,4) ,(0,30) ,(7,0) (8,25)*.

Procedure for Matrix Mapping of Points on Curve

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

1: Convert given message into points on elliptic curve (P)

2: Form Matrix P with mapped points on elliptic curve

3: Compute Q by multiplying P with non-singular matrix (A)

4: Treat resultant values as matrix mapped points (M)

$$P=\begin{bmatrix} P1 & P2 & P3 & \dots & Pw \\ Pw+1 & Pw+2 & Pw+3 & \dots & Ph \\ Ph+1 & Ph+2 & Ph+3 & \dots & Pd \end{bmatrix}$$

$$A=\begin{bmatrix} x11 & x12 & x13 \\ x21 & x22 & x23 \\ x31 & x32 & x33 \end{bmatrix} = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

In step 4, the Multiplication of matrix P and matrix A is performed with addition and doubling of points. M = A*P. This results in another set of points M = $[m_1,m_2\ldots..m_n]$. Figures 7, Figure 8, Figure 9 and Figure 10 shows the RTL Schematic of Implementation of point addition and doubling to perform scalar point multiplication.

The complete mapping and conversion of points are shown in table 4. The matrix de mapping method is same as the matrix mapping method. This method is performed by Multiplication of mapped data with inverse of non-singular matrix. This method retrieves the mapping inputs.

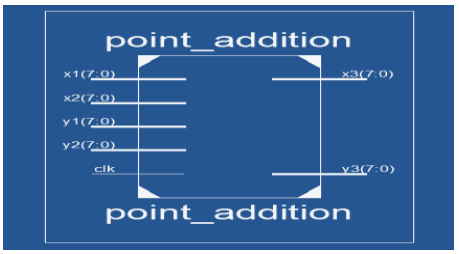


Fig.7 Point Addition

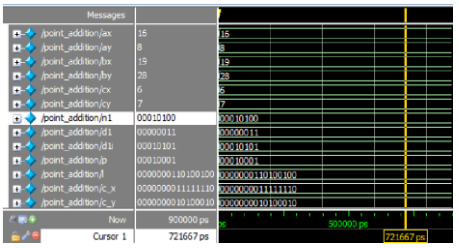


Fig.8 Simulation output of Point Addition

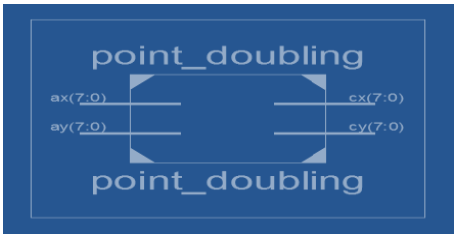


Fig 9. Point Doubling

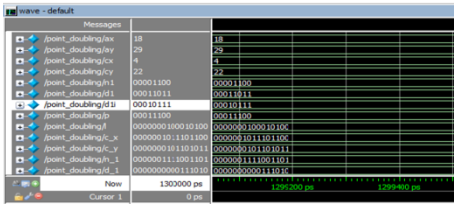


Fig.10 Simulation output of Point Doubling

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

ELGAMAL ALGORITHM

Elgamal Encryption

With sender's key g = 20 and receiver's key k = 16, the encrypted pair of points [C1, C2] are calculated as follows. To find the encrypted points for *'U'*=(25, 15) = Q_i =29*P*.

Encrypted pair of points = ***[C1, C2]*** *=>[(gP), Q_i +k*gP], [20P, Q_i+16*20P] =>* ***[20P, Qi+14P]****=> [(26, 10), Qi + (14P)]=>* ***[20P, 9P] => [(26, 10), (16, 8)]***

Elgamal Decryption

While message decrypting , receiver determines *k(gP)* from the first fragment of the encrypted couple of points, then subtract it from the second portion to acquire, Q_i + *g(kP)* - *k(gP)* = Q_i + *gkP* - *glP* = Q_i. By using the equation $D = (C_2 - kC_1)$ decrypted points can be discovered. To find the decrypted point for *'X'*, *i.e.,* the decrypted point is ***[D7] => (C_2-kC_1) => [(18P – 16(20P)] => [(18P – 14P] => 4P => (4, 22)***.

KNAPSACK ALGORITHM

This algorithm is the most efficient algorithm for the security of the data transmission over an internet. Knapsack cryptography is an important class of public-key cryptosystems in the area of public-key cryptography. It involves no expensive modular exponentiations, which makes the encryption and decryption much more efficient than discrete logarithm based and factorization based cryptosystems. For a long time, knapsack-type cryptosystems were considered to be the most attractive and the most promising due to their high speed of encryption and decryption and NP-completeness nature. Many knapsack type cryptosystems were developed in the history of knapsack public-key cryptography especially in the 1980s, and the cryptographic applications of some variants of the knapsack problem were also investigated [16].

The **Pseudo code for** knapsack algorithm is written below.

Knapsack algorithm consisting of two steps one is ECC encryption with Elgamal algorithm and second one is knapsack process on ECC encrypted data.

Pseudo code for Knapsack Decryption Process consisting of ECC decryption with Elgamal algorithm, followed by knapsack process on ECC encrypted data is given in Table 2.

Table 2.Knapsack Encryption Process

Pseudo code for Knapsack Encryption Process

// First level of Encryption

$Q_i(x,y)+k*gP(x,y)$= (x2,y2)
$k(gP(x,y))$= (x1,y1)

//Second level of Encryption

$$S[x_1] = \sum_{i=1}^{m} a_i x_i.$$

$$a_i = 1, n, n_2, n_3, \cdots, n_m 1 \leq i \leq m.$$

$$x_i = b_1, b_2, \cdots, b_m 1 \leq i \leq m.$$

m is the length of the binary bit string.
p is a prime integer used in the modular arithmetic
k is the secret integer.

S[x1] = Knapsack value (x1);
S[y1] = Knapsack value (y1);
S[x2] = Knapsack value (x2);
S[y2] = Knapsack value (y2);
Cm=((S[x1], S[y1]), (S[x2], S[y2]));

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

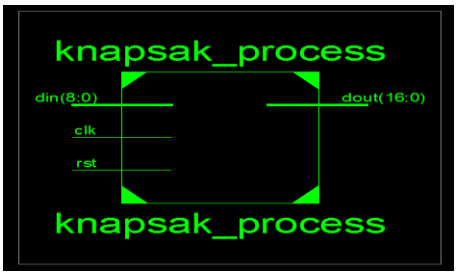


Fig.11 RTL Schematic of Knapsack Process

The plain text input to the knapsack module is 8 bit data as given in Figure 11 and Figure 12. The output is 17 bits, which is taken as input to the Inverse knapsack module as shown in Figure 11 and the process is explained in Table 3.

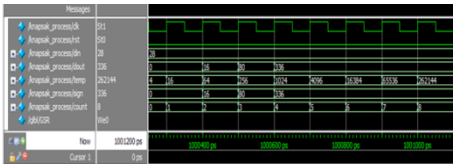


Fig.12 Knapsack process result

Table 3.Knapsack Decryption Process

Pseudo code for Knapsack Decryption Process
// First level of Decryption with Inverse Knapsack Process
$S[x_1] - n^m.$
N[x1] – n^m, is +ve, binary bit is assigned to 1.
N[x1] - $n^m > 0$, binary bit is assigned to 1.
N[x1] - $n^m < 0$, is –ve , binary bit is assigned to 0.

x1 = Inverse Knapsack value (S[x1]);
y1 = Inverse Knapsack value (S[y1]);
x2 = Inverse Knapsack value (S[x2]);
y2 = Inverse Knapsack value (S[y2]);

// Second level of Decryption *l*P(x,y) = (x1,y1);*
$Q_t + l*(k*P(x,y) - k*(l*P(x,y)) = (x2,y2);$

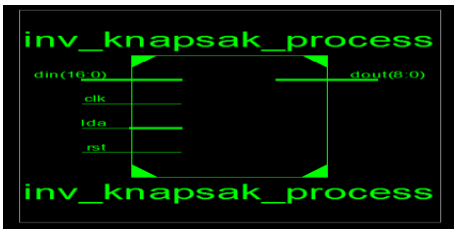


Fig.13 RTL Schematic of Inverse Knapsack Process

The 17 bit cipher text input to the Inverse knapsack module as given in Figure 13 and Figure 14. The output is 8 bits and the process is explained in Table 3.

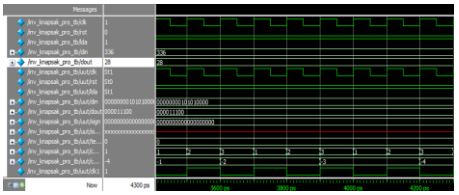
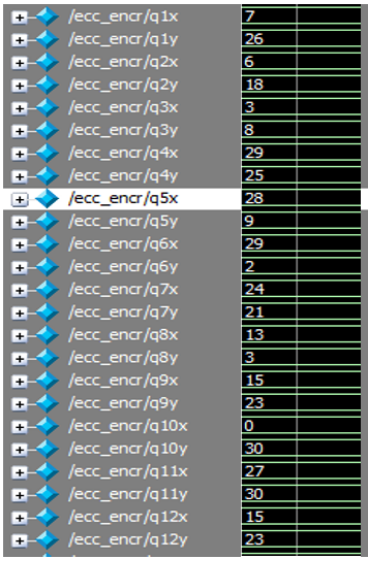


Fig.14 The inverse knapsack process result

COMPUTATIONAL AND IMPLEMENTATION DETAILS



Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

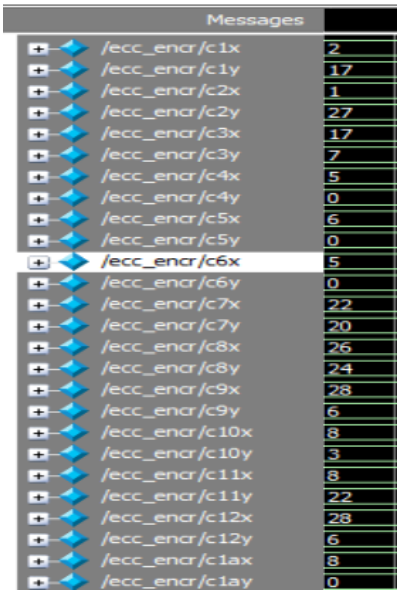
Fig 15. Elgamal Encryption inputs

Fig.16 Elgamal Encryption outputs

The outputs shown in Figure 15 and Figure 16, consists of two co- ordinates (x1,y1) = (cax , cay) and (x2,y2) = (cx, cy). (cx,cy) has 12 outputs for 12 characters and (cax,cay) is same output for all the 12 characters. (cax, cay) = (8,0) and (cx,cy) = (2,17) ,(1,27), (17,7), (5,0), (6,0), (5,0), (22,20), (26,24), (28,6), (8,3), (8,22), (28,6).

The Figure 17 and Figure 18 show the output of integrated module. It consists of point generation module, matrix based mapping module, knapsack encryption module, knapsack decryption module and matrix based de mapping, inverse point generation.

Input text is *"CRYPTOGRAHY"* that can be mapped into points on elliptical curve. Input is 8 bit encrypted data is 17 bit. *(cx, cy)* encrypted points are *(4,257) ,(1,325), (257,21), (17,0), (20,0), (17,0), (276,272) ,(324,320) ,(336,20), (64,5) ,(64,276) ,(336,20)* and (c_{ax}, c_{ay}) points are *(64,0).*



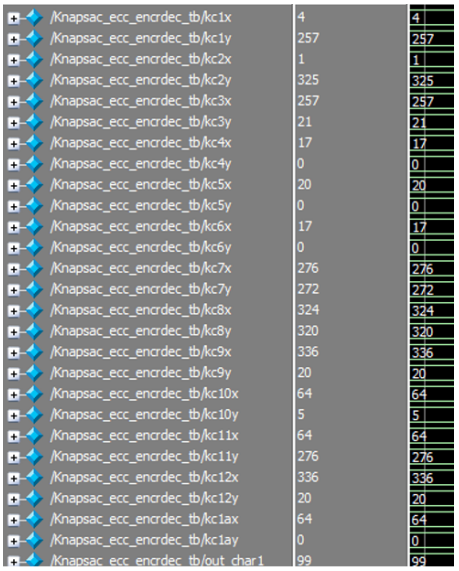


Fig 17. The Encrypted data's of Knapsack encryption and decryption top module

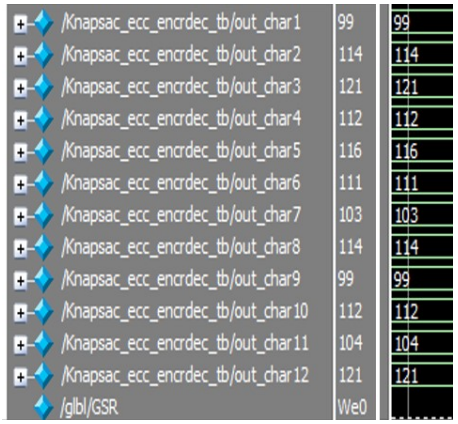


Fig.18 The Knapsack encryption and decryption top module outputs

After decryption the original message "CRYPTOGRAPHY" is retrieved. Figure 11 gives Knapsack encryption and decryption module inputs. Figure 18 is Knapsack encryption and decryption module outputs.

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

Table 5 gives the device utilization for the different processes involved in the complete operations. In Spartan 3E FPGA device, the Xilinx application run out of memory and cannot simplify the operator module. The LUTs and Slice Registers utilization is very less in Artix and Kintex as compared to Spartan 6; this gives a choice to the application developer to choose the FPGA that provides more space to develop other applications on same FPGA. The time required for the processes are in terms of picoseconds that indicates very less computational time is required for the complete crypto processor compared to previous implementations given in table 1.

Table.4 Encryption and decryption of points with matrix mapping

Character andASCII values	Points	Matrix Mapped points	Encrypted points (Knapsack process)	Decrypted points (Inverse Knapsack Process)	Matrix De mapping Points	Inverse points
C = 99	(23, 19)	(22,4)	(64,0) (4,257)	(22,4)	(23, 19)	C = 99
R =114	(19, 28)	(16,18)	(64,0) (1,325)	(16,18)	(19, 28)	R =114
Y =121	(16, 23)	(9,4)	(64,0) (257,21)	(9,4)	(16, 23)	Y =121
P =112	(19, 3)	(2,25)	(64,0) (17,0)	(2,25)	(19, 3)	P =112
T =116	(26, 10)	(15,24)	(64,0) (20,0)	(15,24)	(26, 10)	T =116
O =111	(5, 9)	(29,2)	(64,0) (17,0)	(29,2)	(5, 9)	O =111
G =103	(6, 24)	(12,24)	(64,0) (276,272)	(12,24)	(6, 24)	G =103
R =114	(19, 28)	(5,27)	(64,0) (324,320)	(5,27)	(19, 28)	R =114
A =99	(9, 10)	(7,4)	(64,0) (336,20)	(7,4)	(9, 10)	A =99
P =112	(19, 3)	(0,30)	(64,0) (64,5)	(0,30)	(19, 3)	P =112
H =104	(24, 29)	(7,0)	(64,0) (64,276)	(7,0)	(24, 29)	H =104
Y =121	(16, 23)	(8,25)	(64,0) (336,20)	(8,25)	(16, 23)	Y =121

PERFORMANCE EVALUATION AND DISCUSSIONS

Elliptic Curve Cryptography provides a secure means of exchanging keys among communicating hosts using the Diffie Hellman Key Exchange algorithm. Encryption and Decryption of texts and messages have also been attempted. This work presents the implementation of ECC by first transforming the message into an affine point on the EC, and then applying the knapsack algorithm on ECC encrypted message over the finite field *GF (p).* In ECC we normally start with an affine point called *Pm(x, y).* This point lies on the elliptic curve. In this work we have illustrated encryption/decryption involving the ASCII value of the characters constituting the message, and then subjecting it to the knapsack algorithm. We compare our proposed algorithm with RSA algorithm and show that our algorithm is better due to the high degree of sophistication and complexity involved. It is almost infeasible to attempt a brute force attack. Moreover only one parameter, namely the Knapsack vector a_i alone needs to be kept secret. On the contrary in RSA, three parameters such as the modulus n, its factors p and q need to be kept secret.

Table.5 Device Utilization for Knapsack process and Point inverse on Spartan 6

Operations And Processes	Device Utilization in percentage					
	Spartan 6		Kintex 7		Artix 7	
	Slice Registers	Slice LUTs	Slice Registers	Slice LUTs	Slice Registers	Slice LUTs
Point generation	2% (83/3584)	2% (153/7168)	0.4% (135/41000)	0.4% (87/82000)	0.1% (112/126800)	0.4% (220/634000)
Point addition	2% (91/3584)	2% (165/7168)	0.4% (144/41000)	0.4% (95/82000)	0.1% (124/126800)	0.4% (240/634000)
Knapsack Encryption decryption	3% (112/3584)	3% (220/7168)	0.4% (189/41000)	0.4% (187/82000)	0.1% (212/126800)	0.4% (289/634000)
Inverse Knapsack process	2% (80/3584)	2% (150/7168)	0.4% (130/41000)	0.4% (132/82000)	0.1% (202/126800)	0.4% (265/634000)

Table 6. Timing details

Minimum Period	1.985 ηseconds
Maximum Frequency	503.702MHz
Minimum input arrival time	1.872 ηseconds
Maximum output required time	0.511 ηseconds
Maximum combinational path delay	**No path delay found**

The arrival of this development environment has addressed a number of the widespread concerns relating to WSNs [28][29][30][31]:

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

Strength of Security: The architecture that has been implemented is on a par with previous implementations with respect to area, delay and speed.

Scalability: Key management has been of great concern in WSNs. The mechanism of ECC reduces concerns regarding key management.

Resource Consumption: Considering the ideals of WSNs in relation to one-use devices, this is within the bounds of acceptability. There is provision for improvement in the area.

Speed/Efficiency: There is no combinational path delay; however this may differ with larger data and key size.

The input data of smaller size is used to check for suitability for Wireless Sensor Nodes and since the matrix calculation requires more computation time. The implementation of LUT in coding design becomes complex. As the bit size increases; memory requirement becomes more as affects the energy utilization in networks, thereby network lifetime. We can manipulate data with dissimilar representation to provide protection along with knapsack.

CONCLUSIONS

Utilization of shorter key length in ECC is highly suitable for the user by consuming less power, minimum area and minimum bandwidth. Because of its hardware realization and software efficiency ECC is more efficient than RSA. In this work, a matrix mapping methodology and knapsack algorithms are implemented. In matrix mapping procedure transfer all alphabetic character into points on elliptic curve is defined. Encryption and decryption of mapping points is employed through knapsack algorithm. In mapping method there is complicated to guess the words through it does no longer show any regularity and knapsack algorithm avoids brute force attack by growing confusions. The language used to code these modules is Verilog. The modules are integrated to receive matrix mapping, Knapsack encryption, knapsack decryption and de mapping. The complete crypto process is executed with frequency of 503.702MHz. No Maximum combinational path delay is found in the implementation of modules. In comparison with previous works the area utilization and computational time required in this work is very less, thus satisfying the resource constraints' of wireless sensor nodes.

REFERENCES

Ian, F., Akylidiz, Weilian Su, Yogesh Sankarasubramaniam and E Cayirci.(2002), "Wireless Sensor Network : A Survey on Sensor Networks," *in IEEE Communication Magazine,* ISSN:0163-6804, vol. 40, no. 8, pp. 102-114.

William Stallings. (2011), "Cryptography and network security principles and practices", Prentice Hall, 5th Edition.

Darrel R. Hankerson, A. Menezes and A. Vanstone.(2004), "Guide to Elliptic Curve Cryptography" Springer.

Leif Uhsadel, Markus Ullrich, Amitabh Das, Dusko Karaklajic, Josep Balasch, Ingrid Verbauwhede, Wim Dehaene, "Teaching HW/SW Co-Design With a Public Key Cryptography Application," in IEEE Transactions in Education, 56(4):478-483, 2013.

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

Thomas Newe. (2008), "The Impact of Java and Public Key Cryptography in Wireless Sensor Networking", 2008 The Fourth International Conference on Wireless and Mobile Communications, 07/2008.

Antonio de la Piedra, An Braeken, AbdellahTouhafi.(2012), "Sensor Systems Based on FPGAs and their Applications: A Survey," in Journal of Sensors, DOI:10.3390/s 120912235, 12(0):12235-12264, 2012.

Shaila K, S H Manjula, Thriveni J, Venugopal K R and L M Patnaik.(2011), "Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks ," *in International Journal on Computer Science and Engineering,* ISSN:0975- 3397, vol. 11, no. 3, pp. 31-41.

Lata B T, Vidya Rao, Sivasankari H, Tejaswi V, Shaila K, Venugopal K R, L M Patnaik.(2015), "SEAD: Source Encrypted Authentic Data for Wireless Sensor Networks," *in International Journal of Engineering Research and Development,* e-ISSN: 2278-067X, p-ISSN: 2278-800X, vol. 11, no. 3, pp. 01-16.

Sujoy Sinha Roy and Chester Rebeiro.(2013), " Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* ISSN:1063-8210, vol. 21, no. 5, pp. 901-909.

Hilal Houssain, Mohamad Badra and Turki F Al-Somani.(2012), " Comparative Study of Elliptic Curve Cryptography Hardware Implementations in Wireless Sensor Networks," *in International Journal of RFID Security and Cryptography (IJRFIDSC),* vol. 1, no. 1/2, pp. 67-74..

Kaleel Rahuman and G Athisha.(2010), "Reconfigurable Architecture for Elliptic Curve Cryptography," *in Proceedings of the IEEE International Conference on Communication and Computational Intelligence,* INSPEC Accession number 1188746, pp. 461-466.

A Kaleel Rahuman and G Athisha.(2013), "Reconfigurable Architecture for Elliptic Curve Cryptography using FPGA," *in Mathematical Problems in Engineering, Hindawi Publishing Corporation,* Article ID 675161, 8 pages.

Hassan M N and Benaissa M, "A Scalable Hardware/Software Codesign for Elliptic Curve Cryptography on PicoBlaze Microcontroller," in *Proceedings of 2010 Symposium on IEEE Circuits and Systems (ISCAS),* p-ISBN:978-1-4244-5308-5, pp. 2111-2114, Paris, 2010.

Xining Cui and Jingwei Yang , "An FPGA Based Processor for Elliptic Curve Cryptography," *in Proc. of International Conference on Computer Science and Information Processing (CSIP),* p-ISBN:978-1-46733-1410- 7, pp. 343-350, Xian, China 2012.

Geetha G, Padmaja Jain (2014.), "Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography",

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

International Journal of Computer Applications Technology and Research Volume 3, Issue 5, 312 – 317.

Jitendra Sharma and Prashant Shukla(2013), "ECC Cipher Processor Based On Knapsack Algorithm",National Conference on Emerging Trends in Electrical, Instrumentation &Communication Engineering Vol.3, No.2, pp 67-71.

O.Srinivasa Rao, Prof. S. Pallam Setty.(2010), "Efficient Mapping methods for Elliptic Curve Cryptosystems" , International Journal of Engineering Science and Technology, 2010

F. Amounas and E.H. El Kinani. (2012), "Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography," International Journal of Information & Network Security (IJINS), Vol.1, No.2, pp. 54~59, ISSN: 2089- 3299.

Kamalakannan, V., and S. Tamilselvan. (2015), "Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem", Procedia Materials Science.

G. Chen, G. Bai, and H. Chen.(2007)," A High-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit," IEEE Transactions on Circuits System- II,vol.54,no.5,pp.412-416.

.

E. El Kinani.(2012), "Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography", in International Journal of Information and Network Security (IJINS), vol. 1, no. 2. pp.45-53.

F. Amounas and E.H. El Kinani.(2012), "An Efficient Elliptic Curve Cryptography protocol Based on Matrices", International Journal of Engineering Inventions.

Balamurugan, R., V. Kamalakannan, Ganth D. Rahul, and S. Tamilselvan. "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography", 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014.

Brian King, "Mapping an Arbitrary Message to an Elliptic Curve When Defined Over GF (2^n)," in International Journal of Network Security, 8(2):169-176, 2009.

Anjan K, Abhijith C, Arun Raj, Deekshith, Jibi Abraham, "Design and Mathematical Model of Hybrid Cryptographic Algorithm-A3D Algorithm," in International Journal of Advanced Research in Computer and Communication Engineering, 3(6):6988-6901, 2014.

Fatima Amounas, El Hassan El Kinani, Moha Hajar," A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-Matrix," in International Journal of Engineering and Innovative Technology (IJEIT) Volume 3(1):500-504, 2013..

Jitendra Sharma, Prashant Shukla," ECC Cipher Processor Based On Knapsack Algorithm", in journal of control systems and Informatics, ISSN 2224-5774

Author: - Leelavathi Gopalakrishna, Dr. Shaila K., Dr. Venugopal K.R VTU-Research Centre, India
GARI Publisher | Networks | Volume: 04 | Issue: 03
Article ID: IN/GARI/ICET/2018/106 | Pages: 81-106 (26)
ISSN 2424-6492 | ISBN 978-955-7153-00-1
Edit: GARI Editorial Team | Received: 18.05.2018 | Publish: 15.06.2018

(print) ISSN 2225-0492 (online) ,3(2):53-57, No.2, 2013.

Leelavathi G, Shaila K, Venugopal K R, "Elliptic Curve Cryptography Implementation on FPGA using Montgomery Multiplication for Equal Key and Data size over GF(2m) for Wireless Sensor Networks," in Proceedings of the International Conference on 2016 IEEE Region 10 Conference (TENCON), DOI: 978-1-5090-2597-8/16, pp.469-473, Singapore,2016..

Leelavathi G, Shaila K, Venugopal K R, "Implementation of ECC on FPGA using Scalable Architecture With equal Data and Key for WSN," in International Journal of Engineering and Technology (IJET), ISSN (Print): 2319-8613, ISSN(Online):0975-4024, DOI: 10.21817/ijet/2017/v9i2/170902063, 9(2):773-796, 2017.

Mostafa.I.Soliman, Ghada.Y.Abozaid, " FPGA Implementation and Performance Evaluation of a high throughput Crypto Processor", Elsevier Journal of Parallel and Distributed Computing, 71(2011)1075-1084..

Md Selim Hossain1 , Yinan Kong1, Ehsan Saeedi1, Niras C. Vayalil1, "High-performance elliptic curve cryptography processor over NIST prime fields", IET Journal Computers & Digital Techniques ,2017, Vol. 11 Iss. 1, pp. 33-42.