Vol 06, Article 07608; June 2015
http://ijves.com

International Journal of VLSI and Embedded Systems-IJVES
ISSN: 2249 – 6556

FPGA Based Implementation of Scaling Method for Curve Based Cryptography

SHWETHA M.N, LEELAVATHI
[1]VLSI Design &Embedded Systems, UTL Technologies Limited, VTU Extension Center, Bangalore, India

ABSTRACT

The encryption and decryption algorithms in Elliptic Curve Cryptography (ECC) perform operations only on the curve, but not on the message. Thus, the major task is to transform the given data into points on an elliptic curve. A new scaling method based on matrix properties is presented in the paper which guarantees the confidentiality of messages and raises the potency of elliptic cryptosystem. This includes the mapping of both alphabetic and some special characters onto the points of elliptic curve in the proposed scheme by using non-singular matrix. Later, the mapped points are encrypted/decrypted using Elgamal algorithm. The design focuses on hardware-level of cryptosystems, operating over prime fields GF(p). The final design was implemented using Verilog, simulated and synthesized on FPGA.

Keywords: *Scaling method, FPGA, Curve based cryptography*

[1] INTRODUCTION

Many studies have been carried on Elliptic Curve Cryptosystems (ECC) mechanism, based on public-key (asymmetric)[1] and Tifinagh characters[2], shown in figure 1. Some of them have used the matrix inversion thoroughly to transform the messages in a confidential and secured way[3]. Thus elliptic curves have raised an increasing interest. In addition, a mathematical tool is used to set up new asymmetric schemes, which allow the functionalities like public-key encryption, digital signature, key agreements etc[4]. Compared to other cryptography systems like Rivest-Shamir-Adleman (RSA), one can use an Elliptic Curve group, which maintains the same level of security[5]. Consequently, highly desired properties are exhibited such as less processing power, storage, band width and power consumption[6].

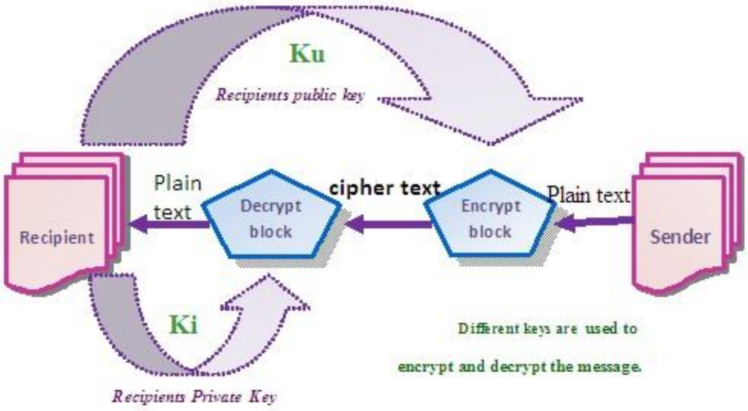

Figure 1: Encryption / Decryption process in asymmetric cryptography

In the static (existing) method, deciphering is easy by using letter frequency attack, because of the simple scaling preserve letter frequencies of the plaintext message [7, 8]. In the proposed method, the same characters are scaled to different points. By this the hidden letter frequencies of the plaintext message are retrievable. Also in this case, we transformed the message into an affine point instead of projective. Encryption/decryption of a transformed character is carried using Elgamal technique. The implementation is focused on a field programmable gate array (FPGA) design and analysis using the Chip-Scope-Pro. Design is created using the hardware description language (HDL-Verilog), to dump on FPGA and XILINX ISE 13.2 simulator is further used to carry the hardware description to implement it, using its knowledge of the gates available on the FPGA.

2. CRYPTOGRAPHY WITH ELLIPTIC CURVE

Elliptic Curve Cryptosystems is one of the powerful tools with RSA and is based on the mathematics of elliptic curves that uses the set of points on an elliptic curve to encrypt / decrypt the data. Because of this, the system becomes infeasible to solve mathematical computations. ECC is first proposed by Victor Miller of IBM and Neal Koblitz in the mid 1980's. ECC is a cryptographic standard, accepted by the National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI) and Federal Information Processing Standard. The hierarchy of ECC operating levels is illustrated in figure 2. ECC is an extreme successor to the RSA and discrete logarithm systems in the future[9].

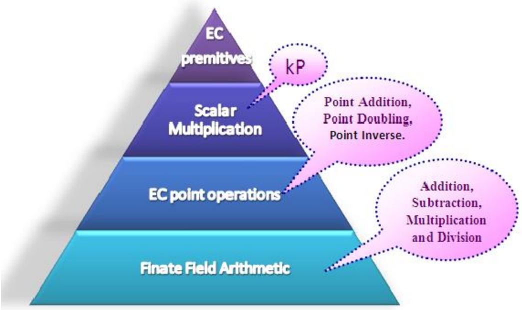
EC premitives
kP
Scalar Multiplication
Point Addition, Point Doubling, Point Inverse.
EC point operations
Addition, Subtraction, Multiplication and Division
Finate Field Arithmetic

Figure 2: Hierarchy of Elliptic Curve Cryptography

In elliptic curve cryptography, we are interested with a restricted form of elliptic curve that is defined over a finite field F_p. The specific concern is the elliptical group mod p, where p is a prime number. Equation 1 defines the conditions for choosing the elliptical curve (where m and n as non-negative integers and should be less than p). Then F_p (m, n) denotes the elliptic group mod p whose elements (x, y) are pairs of non-negative integers less than p. Equation 2 refers to the general form of elliptic curve, both with the point at ∞.

$$4m^3+27n^2 \,|p| \neq 0 \qquad (1)$$

$$y^2=[x^3+mx+n] \,|p| \qquad (2)$$

2. 1 ECC point operations: The concerned point operations are scalar multiplication, point addition, point doubling. The rules for these are explained by many authors [10, 11].

2. 2 ECC Encryption and Decryption

In the present scenario, several algorithms exist to encrypt/decrypt the data using elliptic curves. The work carried is based on one of such methods, known as Elgamal cryptosystem [12]. The primary task in this system is to encode the plaintext "u" to be sent as an x-y point "P_u". P_u is the point that will be encrypted as a cipher-text and subsequently decrypted (deciphered-text).

Let us consider that we have some elliptic curve "C" defined over a finite field "F_p". The point P belongs to "C" is publicly known, as it is the converting system of 'u' to P_u, which embed plain text on an elliptic curve C. If sender wants to communicate with receiver, continuously and securely, they should rely on the following:

Step 1. Receiver selects a random integer k, and issues the point kP (while 'k' remains secret).

Step 2. Sender choose his own random integer g and sends the pair of points (gP, Q_i + g(kP)) to receiver.

Step 3. To decrypt the message, receiver calculates k(gP) from the first part of the pair, then subtracts it from the second part to obtain $\mathbf{Q_i + g(kP) - k(gP) = Q_i + gkP - gkP = Q_i}$ **,** and then contrast the conversion to get back the message.

3. Description of the proposed Method

3.1 Points selection on curve:

The work is carried using the equation of ECC curve given as eqn 2, by considering m=1, n=13, p=31. To find the points on elliptic curve, the following steps are considered.

Step 1: For y= 0 to 31, reckon y^2 |31|.

Step 2: similarly, computed $y^2 = (x^3+x+13)$ |31|, for x= 0 to 31.

Step 3: Match the values of y^2 obtained in step 1 & 2.

Step 4: If it's equal, then the pair (corresponding x and y) becomes a point on an elliptic curve (table 1). For the ECC curve, 34-points can be obtained including point at ∞. If "b" is the base point of the group, then it represents 'A', 2P represents 'B', 3P represents 'C' and so on[13].

Table 1: Set of points on an elliptic curve

P=(9, 10)	2P=(18, 29)	3P= (23, 19)	4P= (4, 22)	5P= (25, 16)
6P=(17,18)	7P= (6, 24)	8P= (24, 29)	9P= (16, 8)	10P= (20, 2)
11P=(22, 22)	12P= (28, 13)	13P= (27, 10)	14P= (26, 21)	15P= (5, 9)
16P=(19, 3)	17P= (10, 0)	18P= (19, 28)	19P= (5, 22)	20P= (26, 10)
21P=(27,21)	22P= (28, 18)	23P= (22, 9)	24P= (20, 29)	25P= (16, 23)
26P=(24, 2)	27P= (6, 7)	28P= (17, 13)	29P= (25, 15)	30P= (4, 9)
31P=(23, 12)	32P= (18, 2)	33P= (9, 21)	∞	

3.2 Matrix Scaling

In the proposed scheme, projection of a new scaling method based on matrices and elliptic curve is discussed. The alphabetic & some special characters are scaled on to the points of the elliptic curve. Both the sender and receiver concur upon some common relationships among them, as follows.

C(F_p): the set of points on elliptic curve.

b: generator(base) point of the curve with order N.
S: the set of all alphabets, including some special characters.
T: the set of the mapping points generated by the proposed algorithm.
X: is non-singular and has only integer entries.
X^{-1} : inverse of matrix X.
k : receivers private key
g : senders secret key
Steps to be followed:

Step 1. Translation of the alphabetic characters into points on elliptic curve.
$[P_1(x_1,y_1), P_2(x_2,y_2),\ldots\ldots, P_d(x_d,y_d)]$
Let us consider that sender wishes to send a message **"VTU EXTENSION CENTRE, UTL, BLR"** to receiver. So, we have P = (9, 10), m= 1 and n = 13. The above message is converted into a stream of points, as following. { (17, 13), (28,18), (26, 10), (27, 21), (4, 9), (25, 16), (20, 29), (26, 10), (25, 16), (16,8), (5, 22), (16, 8), (5, 9), (26,21), (4, 9), (23, 19), (25, 16), (26, 21), (26, 10), (19, 28), (25, 16), (23, 12), (27,21), (26, 10), (28, 13), (23, 12), (18, 29), (28, 13), (19, 28), (17, 13) }
Let 'u' be the original message of length d. If d is not divided by 3, then the points have been padded with ∞, which represent space.
Step 2. Create the matrix of 3*w with entries are points on EC. Here, take w= d/3 and h = 2d/3.

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

Step 3. A non singular matrix of 3*3 such that |A| = ±1 is selected. Using addition and doubling of points to compute: **Q = XU**

$$\text{Where } X = \begin{bmatrix} x11 & x12 & x13 \\ x21 & x22 & x23 \\ x31 & x32 & x33 \end{bmatrix}$$

Step 4. An outcome is set of points T: $T = [Q_1(x_1,y_1), Q_2(x_2,y_2),\ldots\ldots, Q_d(x_d,y_d)]$
Once the characters are scaled onto the curve, these points are crypted using Elgamal encryption/decryption technique.

Step 5. To retrieve the original message, the decrypted points are arranged into a matrix D of 3*10. Finally decoding is performed using the formula **$U = X^{-1} D$ (table 2).**

4. ILLUSTRATION AND RESULTS

4.1 ILLUSTRATION

Taken non-singular matrix X, with sender's private key g = 12 and receiver's private key k = 24 is

$$X = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

and its inverse is, $$X^{-1} = \begin{bmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{bmatrix}$$

Now Q = XU exhibits mapping points, Encrypted points as (E_1,E_2) i.e. $(gP, Q_i+g(kP))$, Decrypted points as $(E_2\text{-}kE_1)$. Get back the original message from decrypted points(D) with the use of inverse matrix of X. i.e., $U = X^{-1}D$.

Table 2. Conversion of Points to Encrypted and Decrypted values.

Characters	Point Pu	Mapping Points(Qi)	Encrypted Points(E1 E2)	Decrypted Points
“	(17, 13)	(17, 13)	(26, 10) (24, 29)	(17, 13)
V	(28, 18)	(24, 2)	(26, 10) (17, 18)	(24, 2)
T	(26, 10)	∞	(26, 10) (26, 21)	∞
U	(27, 21)	(25, 15)	(26, 10) (16, 8)	(25, 15)
space	(4, 9)	(17, 18)	(26, 10) (26, 10)	(17, 18)
E	(25, 16)	(27, 10)	(26, 10) (6, 7)	(27, 10)
X	(20, 29)	(9, 21)	(26, 10) (27, 10)	(9, 21)
T	(26, 10)	(4, 22)	(26, 10) (19, 28)	(4, 22)
E	(25, 16)	(16, 8)	(26, 10) (22, 9)	(16, 8)
N	(16, 8)	(26,21)	(26, 10) (17, 13)	(26,21)
S	(5, 22)	(19, 28)	(26, 10) (18, 2)	(19, 28)
I	(16, 8)	∞	(26, 10) (26, 21)	∞
O	(5, 9)	(17, 13)	(26, 10) (24, 29)	(17, 13)
N	(26, 21)	(26, 21)	(26, 10) (17, 13)	(26, 21)
Space	(4, 9)	(26, 21)	(26, 10) (17, 13)	(26, 21)
C	(23, 19)	(18, 29)	(26, 10) (19, 3)	(18, 29)
E	(25, 16)	(27, 21)	(26, 10) (9, 10)	(27, 21)
N	(26, 21)	(17, 13)	(26, 10) (24, 29)	(17, 13)
T	(26, 10)	(4, 9)	(26, 10) (20, 2)	(4, 9)
R	(19, 28)	(24,2)	(26, 10) (17, 18)	(24,2)
E	(25, 16)	(22, 22)	(26, 10) (16, 23)	(22, 22)
,	(23, 12)	(25, 16)	(26, 10) (5, 22)	(25, 16)
U	(27, 21)	(27, 21)	(26, 10) (9, 10)	(27, 21)
T	(26, 10)	(16, 23)	(26, 10) (25, 16)	(16, 23)
L	(28, 13)	(17, 18)	(26, 10) (26, 10)	(17, 18)
,	(23, 12)	(19, 28)	(26, 10) (18, 2)	(19, 28)
B	(18, 29)	(23, 19)	(26, 10) (10, 0)	(23, 19)
L	(28, 13)	(24, 29)	(26, 10) (28, 18)	(24, 29)
R	(19, 28)	(16, 8)	(26, 10) (22, 9)	(16, 8)
“	(17, 13)	(20, 2)	(26, 10) (19, 28)	(20, 2)

4.2 RESULTS

The design is carried out in XILINX ISE 13.4 simulator. The hardware implementation is carried using Vertex 5 and analysed using Chip-Scope-Pro. The RTL schematic, Scaling, Encryption, Decryption, Decoding of corresponding blocks are shown Figures 3 to 7. In the design, possibilities of sending the characters at once are 30. After scaling, the resultant data is send to the encryption block. Encryption/Decryption can be achieved by using Elgamal method. By using inverse of matrix which was used in scaling and decrypted points Decoding can be obtained. Simulation result of final design is shown in Figure 8.

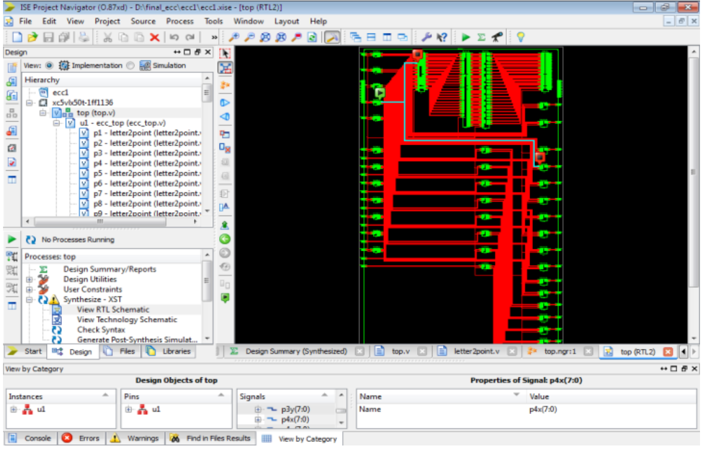
ISE Project Navigator (O.87xd) - D:\final_ecc\ecc1\ecc1.xise - [top (RTL2)]
File Edit View Project Source Process Tools Window Layout Help
Design
View: Implementation Simulation
Hierarchy
ecc1
xc5vlx50t-1ff1136
top (top.v)
u1 - ecc_top (ecc_top.v)
p1 - letter2point (letter2point.
p2 - letter2point (letter2point.
p3 - letter2point (letter2point.
p4 - letter2point (letter2point.
p5 - letter2point (letter2point.
p6 - letter2point (letter2point.
p7 - letter2point (letter2point.
p8 - letter2point (letter2point.
p9 - letter2point (letter2point.
No Processes Running
Processes: top
Design Summary/Reports
Design Utilities
User Constraints
Synthesize - XST
View RTL Schematic
View Technology Schematic
Check Syntax
Generate Post-Synthesis Simulat...
Start
Design
Files
Libraries
Design Summary (Synthesized)
top.v
letter2point.v
top.ngr:1
top (RTL2)
View by Category
Design Objects of top
Properties of Signal: p4x(7:0)
Instances
u1
Pins
u1
Signals
p3y(7:0)
p4x(7:0)
Name
Value
Name
p4x(7:0)
Console
Errors
Warnings
Find in Files Results
View by Category

Figure 3: Register Transfer Logic(RTL) Schematic of main module

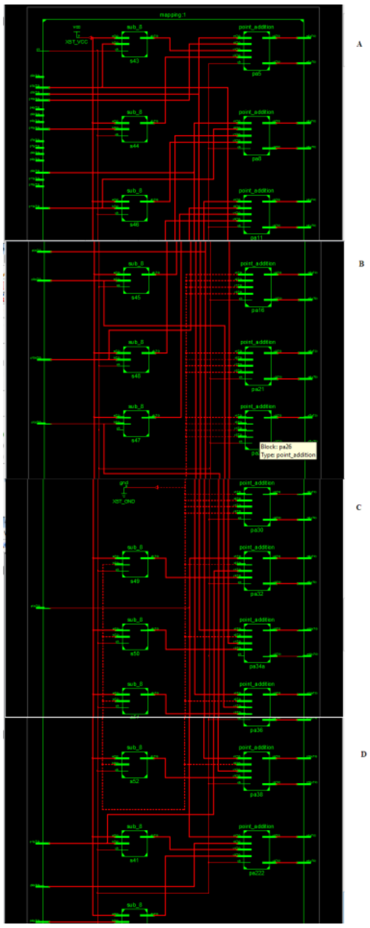

Figure 4 RTL Schematic of scaling

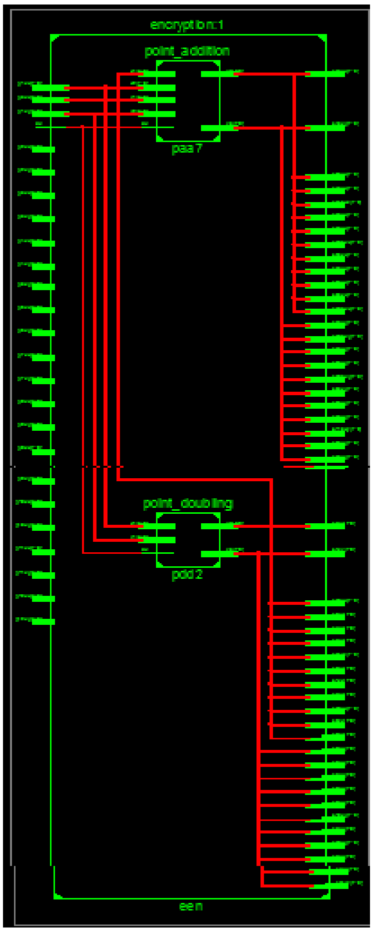

Figure 5: RTL Schematic of encryption block

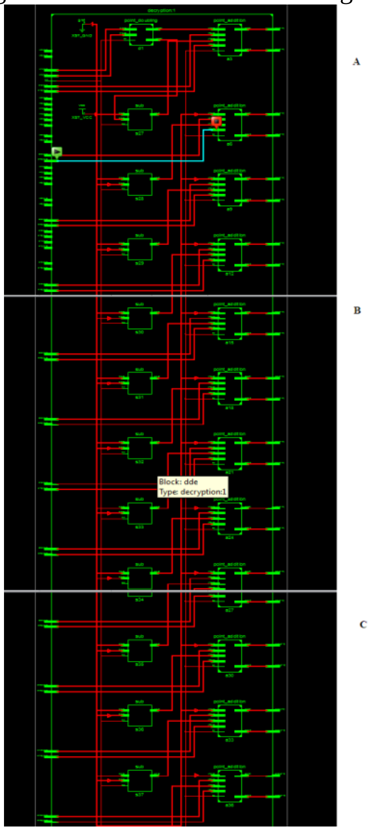

Figure 6: RTL Schematic of decryption block

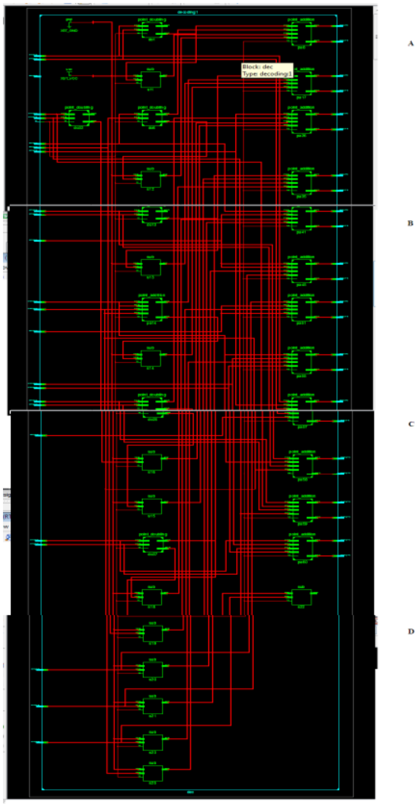

Figure 7: RTL Schematic of decoding block

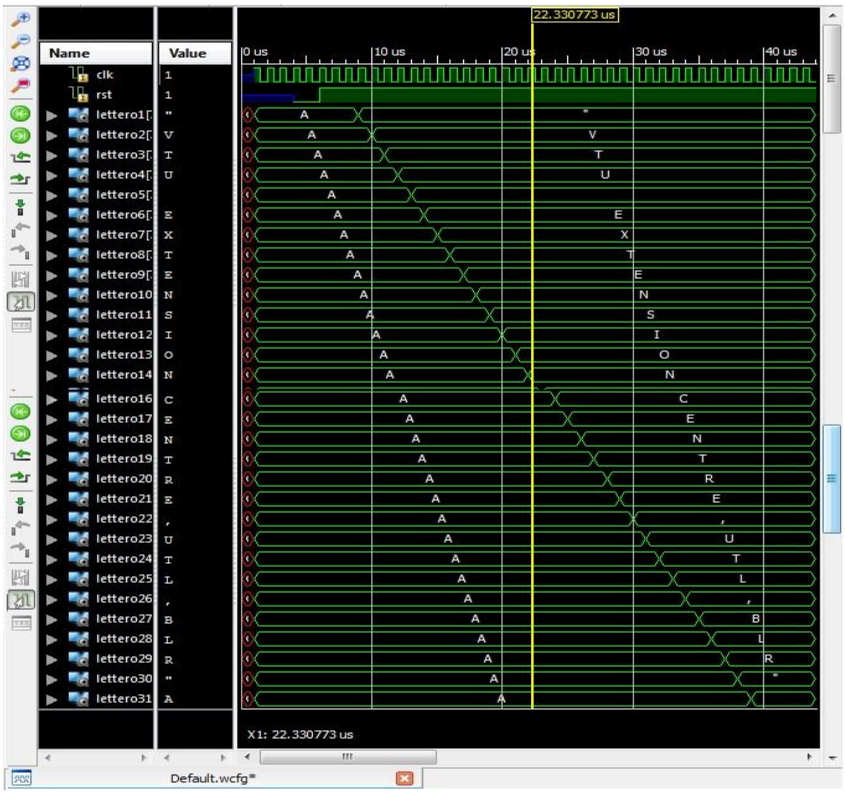

Figure 8: Simulation result of main module

4. CONCLUSIONS

In this paper, we have developed a new method of scaling alphanumeric characters to an EC points by using a non-singular matrix. These mapped points are encrypted and decrypted using ECC (Elgamal) technique. Unlike in conventional method, the gained results indicate that the scaling technique shuns the regularity in the resultant encrypted text which is transformed from plaintext matrix, consequently improves the cumbersomeness of decrypting. i.e, for an encroacher it would be very difficult to hypothesize on which points the alpha-numeric characters are scaled. Therefore, the conclusion is that, the proposed scaling method can reinforce the system, by assuring the confidentiality of data and the improved performance.

ACKNOWLEDGEMENTS

The authors would like to thank the support by Ms. Geetha, Mr. Viswanath for technical support and suggestions, faculty and colleagues at United Technologies Limited, Bangalore for suggestions and comments on the manuscript.

REFERENCES

[1] "An application of discrete algorithms in asymmetric cryptography ", Amounas. F, El Kinani. E.H and Chillali. A, International Mathematical Forum, Vol. 6, No. 49, pp.2409-2418, 2011.

[2] "Cryptography with Elliptic Curve Using Tifinagh Charecters", Amounas. F and El Kinani. E.H,,Journal of Mathematics and System Science Vol.2, No.2, pp.139-144, 2012.

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

[4] "A public key cryptosystem and a signature scheme based on discrete logarithms", Elgamal. T, IEEE Transactions on Information Theory, Vol.31, pp.473- 481, 1985.

[5] "ECC over RSA for Asymmetric Encryption", Kamlesh Gupta, Sanjay Silakari, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[6] "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment", Vivek Katiyar, Kamlesh Dutta, Syona Gupta, International Journal of Computer Applications (0975 – 8887), Volume 11– No.10, December 2010.

[7] "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", Maria Celestin Vigila. S , Muneeswaran. K, IEEE, pp. 82-85, 2009.

[8] "Encoding and Decoding of a message in the Implementation of Elliptic Curve Cryptography uing Koblitz Method", Padma Bh, Chandravathi. D, Prapoorna Roja. P, International Journal on computer Science and

engineering, pp. 1904-1907, 2010.
[9] "A Comparative Study of Public Key Cryptosystem based on ECC and RSA", Arun kumar, Dr. S.S. Tyagi, Manisha Rana, Neha Aggarwal, Pawan Bhadana, Manav Rachna International University, Faridabad, India, International Journal on Computer Science and Engineering (IJCSE), 2011.
[10] "VHDL Implementation using Elliptic Curve Point Multiplication", Ajay Kumar , Kunal Lala , Amit Kumar, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 6, August 2012
[11] "Addition laws on elliptic curves in arbitrary charecteristics", H. Lange and W. Ruppert, Journal of Algrbra, Vol.107(1), pp.106-116, 1987.
[12] "A public key cryptosystem and a signature scheme based on discrete logarithms", T.Elgamal, IEEE Transactions on Information Theory, Vol.31, pp.473- 481, 1985.
[13] "Fast mapping based on Matrix Approach For Elliptic Curve Cryptography", F. Amounas, E.H. El Kinani Moulay Ismaïl University, Morocco, International Journal of Information & Network Security (IJINS), Vol.1, No.2, June 2012, pp. 54~59, ISSN: 2089-3299.