Plain Text encryption and Decryption using koblitz curves

Dr.O.Srinivasa Rao*, Charan Kumar Akiri**
*Dept. Of CSE, University College of Engineering,-JNTUK, KAKINADA, A.P. India-535 003
**Software Engineer, ADB, Hyderabad,India-520 072

ABSTRACT:
Cryptography is the most important aspect of communication security and is becoming increasingly important as a building block for computer security. The increased use of computer and communication systems by industry has increased the risk of theft of proprietary information. These threats may require variety of counter measures; encryption is a primary method of protecting valuable electronic information. In this paper, we propose a model for text encryption using Koblitz curve cryptography (KCC) for secure transmission of plain text for enhancing the security. In this, every character of plain text message is transformed into the points (xm, ym) of Koblitz curve and then these points are encrypted for secure transmission.The resulting system can be used for security applications in smart cards, personal digital assistance, and wireless devices for enhancing the security.

Keywords- koblitz Curve Cryptography (ECC), plain text, Cipher text, encryption, decryption, smart cards, personal digital assistance, and wireless devices .

I. INTRODUCTION

N. Koblitz[1] and Victor Miller[2], independently proposed the elliptic curve cryptosystem in 1985,is becoming the choice for mobile communication. In 1991, Koblitz[1] suggested special family of elliptic curves popularly known as koblitz curves, which are widely studied in the academia and have been included in certain standard[2-4].

Elliptic curve cipher use very small key size and computationally is very efficient. One can use an elliptic curve group that is smaller in size while maintaining the same level of security. The result is smaller key sizes, bandwidth savings, and faster implementations—features that are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, personal digital assistants, and wireless devices. Elliptic curve cryptographic protocols for digital signatures, public-key encryption, and key establishment have been standardized by numerous standards organizations including:

- American National Standards Institute (ANSI X9.62 [3], ANSI X9.63 [4])
- Institute of Electrical and Electronics Engineers (IEEE 1363-2000 [5])
- International Standards Organization (ISO/IEC 15946-3 [6])
- U.S. government's National Institute for Standards and Technology (FIPS 186-2 [7])
- Internet Engineering Task Force (IETF PKIX [7], IETF OAKLEY [8])
- Standards for Efficient Cryptography Group (SECG [9])

The vast majority of the products and standards that use public-key cryptography for encryption and digital signatures use RSA [10]. As we have seen, the bit length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. Recently, a competing system that has emerged is elliptic curve cryptosystem (ECC)[4,11].

1.1 Elliptic Curve Cryptography:

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: Prime curves defined over Z_p and binary curves constructed over GF (2^m). Fernandez[12] points out that prime curves are best suited for software applications, as the extended bit –fiddling

operations needed by binary curves are not required; ,and that binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful and fast cryptosystem. In this paper we used koblitz curves defined over (2^m) for analysis purpose.

1.2 Koblitz curves:

A koblitz curve E over F_2^m is an elliptic curve whose defining equation has coefficients in F_2. There are two koblitz curves: $y^2+xy=x^3+1$ and $y^2+xy=x^3+x^2+1$.These elliptic curves were first proposed for cryptographic use by koblitz [13].They have advantages over randomly selected curves over binary fields because the point multiplication operation in Koblitz curves involves no point doubling ([14, 15], [16]).Koblitz curves have been standardized in NIST's FIPS (186-2[2]).

1.3 Elliptic Curves Arithmetic over F_2^m:

A (non-super singular) elliptic curve $E(F_2^m)$ over F_2^m defined by the parameters a,b ϵ F_2^m ,$b \neq 0$, is the set of all solutions (x, y), x, y ϵ F_2^m, to the equation

$$y^2+xy=x^3+ax^2+b,$$

Together with an extra point O, which is the point at infinity. The set of points $E(F_2^m)$ forms a group with the following additional rules:

1. $O+O=O$
2. $(x, y)+O=O+(x, y)=(x, y)$ for all $(x, y)\epsilon E(F_2^m)$.
3. $(x, y)+(x, x + y)=O$ for all $(x, y) \epsilon E(F_2^m)$ (i.e., the negative of the point (x, y) is $-(x, y)=(x, x + y)$).
4. (Rules for adding two distinct points that are not inverse of each other)

Let $P = (x_1, y_1) \epsilon E(F_2^m)$ and $Q=(x_2,y_2) \epsilon E(F_2^m)$ be two points such that $x_1 \neq x_2$.Then

$P+Q=(x_3,y_3)$,where

$x_3=\lambda^2+ \lambda+x_1+x_2+a$,

$y_3= \lambda(x_1+x_3) +x_3+y_1$, and

$\lambda = (y_2+y_1)/(x_2+x_1)$

5. (Rule for doubling a point)

Let $P=(x_1, y_1) \epsilon E (F_2^m)$ be a point with $x_1 \neq 0$. (If $x_1=0$ then P=-P, and so 2P=O)Then $2P =(x_3,y_3)$, where

$x_3= \lambda^2+ \lambda + a$

$y_3=x_1^2+ (\lambda+1) x_3$, and

$\lambda =x_1+ (y_1/x_1)$

II. PROPOSED MODEL FOR TEXT ENCRYPTION AND DECRYPTION

The proposed model at sender and receiver side for text in the context of KCC for enhancing the security in Figure1.The following two sections describes the proposed model at sender side and at receiver side of text encryption by aiming the confidentiality to the data.

2.1 Encryption procedure (at sender side)

1. Take plain text S,
2. Each character of S, i.e. called as message P_m, can be mapped to the point (X_m, Y_m) on chosen Koblitz curve.
3. Encryption/decryption system require a point on G and an elliptic group $E_p(a, b)$. User A select a private key n_A and generate a public key $P_A = n_A$ x G. To encrypt and send pixel P_m, to B, A choose a random positive integer k and produce the cipher text C_m consisting of the pair of points $C_m = \{kG, P_m + kP_B\}$, where P_B is the public key of user B.

2.2 Decryption at the receiver side

To decrypt the cipher Text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

For practical purpose, we have taken koblitz curve of $y^2+xy=x^3+ax^2+b$, in the binary field and an irreducible polynomial of $x^{10}+x+1$. The points on the koblitz curve are shown in the table1.The number of points on the chosen koblitz curve and irreducible polynomials is less than 2^{10} . The alpha numerical characters of the plain text are mapped [17, 18] to these points. The mapped points and encrypted points are shown in the table 2

Table 1

S.No.	Point(x,y)	S.NO.	Point(x,y)

1	{(0,0,0,0,0,0,0,0,0,0),(0,0,0,0,0,0,0,0,0,1)}	958	{(1,1,1,1,1,1,0,1,0,1),(0,1,0,0,0,1,0,0,1,0)
2	{(0,0,0,0,0,0,0,0,0,0),(0,0,1,1,1,0,1,1,0,0)}	959	{(1,1,1,1,1,1,0,1,0,1),(1,0,1,1,1,0,0,1,1,1)}
3	{(0,0,0,0,0,0,0,0,0,1),(0,0,1,1,1,0,1,1,0,1)}	960	{(1,1,1,1,1,1,0,1,1,1),(0,1,0,1,0,1,1,0,1,1)}
4	{(0,0,0,0,0,0,0,0,1,0),(0,0,1,1,1,1,1,0,0,0)}	961	{(1,1,1,1,1,1,0,1,1,1),(1,0,1,0,1,0,1,1,0,0)}
5	{(0,0,0,0,0,0,0,0,1,0),(0,0,1,1,1,1,1,1,0,1,0)}	962	{(1,1,1,1,1,1,1,1,0,1),(0,1,1,1,0,0,0,0,0,1)}
6	{(0,0,0,0,0,0,0,1,0,0),(0,1,1,1,1,1,1,1,0,0,1)}	963	{(1,1,1,1,1,1,1,1,0,1),(1,0,0,0,1,1,1,1,0,0)}
7	{(0,0,0,0,0,0,0,1,0,0),(0,1,1,1,1,1,1,1,1,0,1)}	964	{(1,1,1,1,1,1,1,1,1,0),(0,1,1,0,0,0,0,1,0,1)}
8	{(0,0,0,0,0,0,1,0,0,1),(1,0,0,0,1,0,0,0,1,0)}	965	{(1,1,1,1,1,1,1,1,1,0),(1,0,0,1,1,1,1,0,1,1)}
9	{(0,0,0,0,0,0,1,0,0,1),(1,0,0,0,1,0,1,0,1,1)}	966	{(1,1,1,1,1,1,1,1,1,1),(0,0,1,0,0,1,0,0,0,0)}
---	------	968	{(1,1,1,1,1,1,1,1,1,1),(1,1,0,1,1,0,1,1,1,1)}

Encryption:

S. No.	Plain text	Mapping points	Encrypted text/points
1	APPLE	{[(0,0,0,1,0,0,1,1,1,1),(0,1,1,0,1,0,0,1,1,0)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,1,1,0,0,1,0,0,1,1),(1,0,0,1,0,1,1,0,1,1)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)]}	{[(1,0,0,1,1,1,1,0,0,0),(0,1,0,1,0,0,1,0,0,1)], [(0,0,1,1,1,0,0,1,0,0),(0,1,1,0,1,1,0,1,0,1)], [(0,0,1,1,1,0,0,1,0,0)(0,1,1,0,1,1,0,1,0,1)], [(0,1,1,0,1,0,0,1,0,0),(1,0,1,0,1,1,0,1,0,0)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)]}
2	BARKLEY	{[(1,0,1,1,0,0,1,1,1,1),(1,0,1,1,0,1,0,1,0,1)], [(0,0,0,1,0,0,1,1,1,1),(0,1,1,0,1,0,0,1,1,0)], [(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)], [(0,0,1,0,0,1,0,0,1,1),(0,1,0,1,0,1,0,0,1,0)], [(1,1,1,0,0,1,0,0,1,1),(1,0,0,1,0,1,1,0,1,1)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,1,1,1,0,0,0,1,1),(0,0,1,1,1,1,1,0,0,0)]}	{[(0,0,1,1,1,1,1,0,0,0),(1,0,0,0,1,1,1,0,1,0)], [(1,0,0,1,1,1,1,0,0,0),(0,1,0,1,0,0,1,0,0,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)], [(1,0,1,0,1,0,0,1,0,0),(0,1,1,0,1,1,1,1,0,1)], [(0,1,1,0,1,0,0,1,0,0),(1,0,1,0,1,1,0,1,0,0)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,1,1,0,1,0,1,0,0),(0,0,0,0,0,1,0,1,1,1)]}
3	COMPUTER	{[(0,1,1,1,0,0,1,1,1,1),(0,0,0,1,0,1,0,1,0,1)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,1,0,0,0)], [(0,0,0,1,0,1,0,0,1,1),(1,0,1,1,0,0,1,0,0,1)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,1,1,0,1,0,0,0,1,1),(0,1,1,1,0,0,1,0,0,1)], [(0,1,0,0,1,0,0,0,1,1),(0,0,0,0,0,0,0,0,0,0)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)]}	{[(1,1,1,1,1,1,1,0,0,0(0,0,1,0,1,1,1,0,1,0)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,0,0,1,1,0,0,1,0,0),(1,0,0,0,1,0,0,1,1,0)], [(0,0,1,1,1,0,0,1,0,0),(0,1,1,0,1,1,0,1,0,1)], [(0,1,1,0,0,1,0,1,0,0),(0,1,0,0,1,0,0,1,1,0)], [(1,1,0,0,0,1,0,1,0,0),(0,0,1,1,1,0,1,1,1,1)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)]}
4	DOCTOR	{[(1,1,0,0,1,1,0,0,1,1),(1,1,1,0,0,0,0,0,0,0)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,1,0,0,0)], [(0,1,1,1,0,0,1,1,1,1),(0,0,0,1,0,1,0,1,0,1)], [(0,1,0,0,1,0,0,0,1,1),(0,0,0,0,0,0,0,0,0,0)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,1,0,0,0)], [(0,1,1,1,0,1,0,0,1,1)(1,0,1,1,1,1,1,0,0,0)]}	{[(0,1,0,0,0,0,0,1,0,0),(1,1,0,1,1,0,1,1,1,1)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,1,1,1,1,1,1,0,0,0),(0,0,1,0,1,1,1,0,1,0)], [(1,1,0,0,0,1,0,1,0,0),(0,0,1,1,1,0,1,1,1,1)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)]}
5	ENGINEERING	{[(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)],	{[(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],

		[(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)], [(0,1,0,1,1,1,0,0,1,1),(1,1,0,0,0,0,0,0,0,1)], [(0,0,1,1,1,1,0,0,1,1)(0,0,0,1,0,0,0,0,0,0)], [(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)], [(0,0,1,1,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)], [(0,1,0,1,1,1,0,0,1,1),(1,1,0,0,0,0,0,0,0,1)]}	[(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)] [(1,1,0,1,0,0,0,1,0,0),(1,1,1,1,1,0,1,1,1,0)], [(1,0,1,1,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)], [(1,0,1,1,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)], [(1,1,0,1,0,0,0,1,0,0),(1,1,1,1,1,0,1,1,1,0)]}

Decryption:

S.No.	Encrypted text/points	Decrypted points	Plain text
1	{[(1,0,0,1,1,1,1,0,0,0),(0,1,0,1,0,0,1,0,0,1)], [(0,0,1,1,1,0,0,1,0,0),(0,1,1,0,1,1,0,1,0,1)], [(0,0,1,1,1,0,0,1,0,0)(0,1,1,0,1,1,0,1,0,1)] [(0,1,1,0,1,0,0,1,0,0),(1,0,1,0,1,1,0,1,0,0)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)]}	{[(0,0,0,1,0,0,1,1,1,1),(0,1,1,0,1,0,0,1,1,0)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,1,1,0,0,1,0,0,1,1),(1,0,0,1,0,1,1,0,1,1)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)]}	APPLE
2	{[(0,0,1,1,1,1,1,0,0,0),(1,0,0,0,1,1,1,0,1,0)], [(1,0,0,1,1,1,1,0,0,0),(0,1,0,1,0,0,1,0,0,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)], [(1,0,1,0,1,0,0,1,0,0),(0,1,1,0,1,1,1,1,0,1)], [(0,1,1,0,1,0,0,1,0,0),(1,0,1,0,1,1,0,1,0,0)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,1,1,0,1,0,1,0,0),(0,0,0,0,0,1,0,1,1,1)]}	{[(1,0,1,1,0,0,1,1,1,1),(1,0,1,1,0,1,0,1,0,1)], [(0,0,0,1,0,0,1,1,1,1),(0,1,1,0,1,0,0,1,1,0)], [(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)], [(0,0,1,0,0,1,0,0,1,1),(0,1,0,1,0,1,0,0,1,0)], [(1,1,1,0,0,1,0,0,1,1),(1,0,0,1,0,1,1,0,1,1)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,1,1,1,0,0,0,1,1),(0,0,1,1,1,1,1,0,0,0)]}	BARKLEY
3	{[(1,1,1,1,1,1,1,0,0,0(0,0,1,0,1,1,1,0,1,0)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,0,0,1,1,0,0,1,0,0),(1,0,0,0,1,0,0,1,1,0)], [(0,0,1,1,1,0,0,1,0,0),(0,1,1,0,1,1,0,1,0,1)], [(0,1,1,0,0,1,0,1,0,0),(0,1,0,0,1,0,0,1,1,0)], [(1,1,0,0,0,1,0,1,0,0),(0,0,1,1,1,0,1,1,1,1)], [(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)]}	{[(0,1,1,1,0,0,1,1,1,1),(0,0,0,1,0,1,0,1,0,1)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,1,0,0,0)], [(0,0,0,1,0,1,0,0,1,1),(1,0,1,1,0,0,1,0,0,1)], [(1,0,1,1,0,1,0,0,1,1),(0,1,0,1,0,1,1,0,1,0)], [(1,1,1,0,1,0,0,0,1,1),(0,1,1,1,0,1,1,0,1,0)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,0,0,0,0,0,0,0)], [(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)], [(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)]}	COMPUTER
4	{[(0,1,0,0,0,0,0,1,0,0),(1,1,0,1,1,0,1,1,1,1)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,1,1,1,1,1,1,0,0,0),(0,0,1,0,1,1,1,0,1,0)], [(1,1,0,0,0,1,0,1,0,0),(0,0,1,1,1,0,1,1,1,1)], [(1,1,0,1,1,0,0,1,0,0),(1,1,1,1,1,0,0,1,1,1)], [(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)]}	{[(1,1,0,0,1,1,0,0,1,1),(1,1,1,0,0,0,0,0,0,0)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,1,0,0,0)], [(0,1,1,1,0,0,1,1,1,1),(0,0,0,1,0,1,0,1,0,1)], [(0,1,1,1,0,0,1,1,1,1),(0,0,0,1,0,1,0,1,0,1)], [(0,1,0,0,1,0,0,0,1,1),(0,0,0,0,0,0,0,0,0,0)], [(0,1,0,1,0,1,0,0,1,1),(1,1,0,0,0,0,0,1,0,0)], [(0,1,1,1,0,1,0,0,1,1)(1,0,1,1,1,1,1,0,0,0)]}	DOCTOR
5	{[(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],	{[(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)],	ENGINEERING

	[(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)]	[(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)],	
	[(1,1,0,1,0,0,0,1,0,0),(1,1,1,1,1,0,1,1,1,0)],	[(0,1,0,1,1,1,0,0,1,1),(1,1,0,0,0,0,0,0,0,1)],	
	[(1,0,1,1,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],	[(0,0,1,1,1,1,0,0,1,1)(0,0,0,1,0,0,0,0,0,0)],	
	[(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)],	[(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)],	
	[(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],	[(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)],	
	[(1,1,0,0,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],	[(0,1,0,0,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)],	
	[(1,1,1,1,1,0,0,1,0,0),(1,0,0,0,0,1,0,1,1,1)],	[(0,1,1,1,0,1,0,0,1,1),(1,0,1,1,1,1,1,0,0,0)],	
	[(1,0,1,1,0,0,0,1,0,0),(0,0,1,0,1,0,1,1,1,1)],	[(0,0,1,1,1,1,0,0,1,1),(0,0,0,1,0,0,0,0,0,0)],	
	[(0,1,0,1,1,0,0,1,0,0),(0,1,1,0,0,0,0,1,0,0)],	[(1,1,0,1,0,1,0,0,1,1),(0,1,0,1,1,0,1,0,1,1)],	
	[(1,1,0,1,0,0,0,1,0,0),(1,1,1,1,1,0,1,1,1,0)]}	[(0,1,0,1,1,1,0,0,1,1),(1,1,0,0,0,0,0,0,0,1)]}	

III. CONCLUSION

The experiments are conducted for different input plain text strings and obtained corresponding output cipher texts and vice versa. We conclude that this koblitz curves more efficient than primary curve cryptography and also best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem.

REFERENCES

[1] Neal Koblitz, "Elliptic Curve Cryptosystem, Journal of mathematics computation Vol.48, No.177pp.203-209,Jan-1987.

[2] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology–Crypto '85,Lecture Notes in Computer Science, 218

[3] Certicom Corp., "An Introduction to Information Security", Number 1, March 1997.

[4] ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Elliptic CurveKey Agreement and Key Transport Protocols, ballot version, May 2001.

[5] Internet Engineering Task Force, The OAKLEY Key Determination Protocol, IETF RFC 2412, November 1998.

[6] ISO/IEC 15946-3, Information Technology–Security Techniques–Cryptographic Techniques Based on Elliptic Curves, Part 3, Final Draft International Standard (FDIS), February 2001

[7] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication186-2, 2000.

[8] M. Jacobson, N. Koblitz, J. Silverman, A. Stein and E. Teske, "Analysis of the xedni calculus attack", Designs, Codes and Cryptography, 20 (2000), 41-64. (1986), Springer-Verlag, 417-426.

[9] Standards for Efficient Cryptography Group, SEC 1: Elliptic Curve Cryptography, version1.0, 2000. Available at http://www.secg.org

[10] R.L. Rivest, A. Shamir, and L.M. Adleman, Method for Obtaining Digital Signatures and Public-key Cryptosystems ", Communications of the ACM,Volume 21, pages 120-126, February 1978.

[11] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three", Advances in Cryptology–Asiacrypt 2000, LectureNotes in Computer Science, 1976 (2000),Springer-Verlag, 248-259

[12] Fernandes, A. "Elliptic Curve Cryptography", Dr.Dobb's journal, December 1999

[13] N.Koblitz, CM-curves with good cryptographic properties in: Advances in cryptology, [14]Solinas, "An improved algorithm for arithmetic on a family of elliptic curve", Advances in Cryptology - CRYPTO '97, Lecture Notes in Computer Science, 1997, Volume 1294/1997, 357-371, DOI: 10.1007/BFb0052248 ,1294(1997). Springer-Verlog, 357-371

[15]J.Solinas," Efficient arithmetic on koblitz Curves", Design codes and cryptography, 19(2000), 195-249

[16] Yong-hee Jang, Yong-jin Kwon "Efficient Scalar Multiplication Algorithms Secure against Power Analysis Attacks for Koblitz Curve Cryptosystems" 2010, 10th Annual International Symposium on Applications and the Internet, IEEE Computer Society

[17] Vigila, S.; Muneeswaran, K.; "Implementation of text based cryptosystem using Elliptic Curve Cryptography ", Advanced Computing, 2009. ICAC 2009. First International Conference on 13-15 Dec. 2009,Onpage(s): 82-85.
[18] O.Srinivasa Rao, S.Pallam Setty, "Efficient mapping methods of Elliptic Curve Crypto Systems" International Journal of Engineering Science and Technology, Vol. 2(8), 2010, pp. 3651-3656