Implementation of Elliptic Curve Cryptography for Audio Based Application

Rahul Singh[1], Ritu Chauhan [2], Vinit Kumar Gunjan[3], Pooja Singh[4]

[1, 2] *Sobhasaria Group of Institution, Sikar, Rajasthan, India*
[3] *BioAxis DNA Research Centre, Hyderabad, Andhra Pradesh 500068, India*
[4] *Dot Spiders InfoSolutions (P) Ltd, GautamBuddha Nagar, India*

***Abstract*— Recently 3G technology has grown rapidly and is becoming a medium of choice for communication. All elements of multimedia (text image audio and video) are used. In this era, network security has become an issue of importance, on which a lot of research is going on. This paper presents the implementation of ECC by first transforming the audio file into an affine point on the Elliptic Curve (EC), over the finite field GF(p). In ECC we normally start with an affine point called Pm(x,y) which lies on the elliptic curve. In this paper we illustrate the process of encryption/decryption for audio file. It is almost infeasible to attempt a brute force attack to break the cryptosystem using ECC.**

Keywords: Elliptic Curve Cryptography (ECC), elliptic curve, audio encryption/decryption.

I. INTRODUCTION

Elliptic curves (EC) were suggested for cryptography by Victor Miller [1] and Neal Koblitz [2] in 1985 in the form of Elliptic Curve Cryptography (ECC). ECC follows Public Key encryption technique and the security provided is based on the hardness of Discrete Logarithm Problem (DLP) and since then, a lot amount of work has been done on Elliptic Curve Cryptography. One main advantage of ECC is that similar lever of security can be achieved with considerably smaller keys size.

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. In ECC we normally start with an affine point called Pm(x,y). These points may be the Base point (G) itself or some other point closer to the Base point. Base point implies it has the smallest (x,y) co-ordinates, which satisfy the EC.

Today, RSA is the powerhouse crypto security of choice for E-commerce transaction. The RSA is too slow compared to ECC because ECC required smaller key size. The IT connectivity provides will be able to utilize fewer crypto-server securities for providing secure network connections. Table 1 compares the security level for some commonly considered crypto-graphics Key size.

RSA/DSA key size	ECC key size	RSA/ECC key size ratio
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

Table 1: *Comparison of the equivalent security level for some commonly used cryptographic key sizes.*

II. RELATED WORKS

In the literature, many authors have tried to exploit the features of EC field to deploy for security applications. We have outlined some of the highlights of the relevant work in this section. M.Prabu et al [3] has presented an implementation of ECC over the prime field GF(p) and binary field GF(2^m) along with the performance. Kristin Lauter has provided an overview of ECC for wireless security [4]. It focuses on the performance advantages in the wireless environment by using ECC instead of the traditional RSA cryptosystem. Mohammad Ghamgosar et al., [5] in his work has explained application of ECC in wireless communication security. Yacine Rebahi et al [6] explains the use of ECC in the identity

management for Session Initiation protocol. C. J. McIvor et.al [7] introduces a novel hardware architecture for ECC over GF(p). The work presented by Gang Chen presents a high performance EC cryptographic process for general curves over GF(p) [8]. The standard specifications for public key cryptography is defined in [9] .

A simple tutorial of ECC concept is very well documented and illustrated in the text authored by Williams Stallings et.al [10]. The paper presented by Kevin M. Finnigin et al outlines a brute-force attack on ECC implemented on UC Berkley's Tiny OS operating system for wireless sensor networks [11].

S. V. Sathyanarayana et.al [12] presents Symmetric Key Image Encryption scheme with Key sequences derived from random sequence of cyclic elliptic curve poits. In the paper as proposed by Jaewon Lee [13] presents 3 algorithms to perform scalar multiplication on EC defined over higher characteristic finite fields such as OEA (Optimal Extension Field). Liu Yongliang [14] showed that Aydos et al.' s protocol is vulnerable to man-in the-middle attack from any attacker but not restricted on the inside attacker. They proposed a novel ECC based wireless authentication protocol. A comprehensive coverage of EC field with the in-depth mathematical treatment is given in [15]. Owing to these existing works on ECC and its popularity, it is proposed to implement the crypto system based on ECC for audio based application.

III. MATHEMATICAL REVIEW

Elliptic Curve Cryptography: We consider an elliptic curve over a finite field associated with a prime number p > 3 whose equation can be written as [2]

$y^2 = x^3 + ax + b$ …. (1)

Where a, b are two integers which satisfy $4a^3 + 27b^2 \neq 0 \pmod p$. Then the elliptic group, Ep(a, b), is the set of pairs (x, y), where 0 < x, y < p, satisfying the equation (2) with the point at infinity denoted as O. The basic EC operations are point addition and point doubling defined on the group Ep (a, b) is calculated as follows.

Let A = (x1, y1) and B = (x2, y2) be in Ep (a, b), then A * B = (x3, y3) is defined as

$x3 \equiv S^2 - x1 - x2 \pmod p$

$y3 \equiv S(x1 - x3) - y1 \pmod p$ …… (2)

where

$$S = \begin{cases} \frac{y2-y1}{x2-x1} & \text{if } A \neq B \\ \frac{3x1^2+a}{2y1} & \text{if } A = B \end{cases}$$

An example of $E_{29}(4, 20)$ is given in table2.

∞	(2,6)	(4,19)	(8,10)	(13,23)	(16,2)	(19,16)
(0,7)	(2,23)	(5,7)	(8,19)	(14,6)	(16,27)	(20,3)
(0,22)	(3,1)	(5,22)	(10,4)	(14,23)	(17,10)	(20,26)
(1,5)	(3,28)	(6,12)	(10,25)	(15,2)	(17,19)	(24,7)
(1,24)	(4,10)	(6,17)	(13,6)	(15,27)	(19,13)	(24,22)

Table 2: *Point on the Elliptic Curve $E_{29}(4,20)$.*

IV. THE ENCRYPTION ALGORITHM

1. First we take an audio file as an input X.

2. Each value of audio file X, that is called message m, can be converted into the coordinate (X_m, Y_m) that are the point on elliptic curve .

$$X_m = m*K + J,\ J = 0,1,2,3\ldots$$

$$Y_m = \sqrt{x3 + ax + b}$$

where m is message K is the random positive integer. (Xm,Ym) is a square modulo P, where P is the prime no. and $P \geq K*m$.

3. Encryption/ Decryption system require a point on **G** and an elliptic group **Ep(a,b).** User A chooses a secret integer **s** and computes **Q = s.G**. User B's public key consists of **Ep(a,b),** and the points **G** and **Q**, while the integer **s** is kept private. To encrypt and send message $\mathbf{P_m}$ to user B, user A choose a random positive integer k and produce the ciphertext $\mathbf{C_m}$ consisting of the pair of points.

$$C_m = \{kG, P_m + kQ\}$$

4. Decrypt the ciphertext using the method

$\{P_m + kQ - s.(kG) = P_m + k(s.G) - s.(kG)\}$

$= P_m$

V. RESULTS

We transform different .wav audio file into (Xm, Ym) coordinate that is the point of elliptic curve and then encrypted. Note that the original message will be completely recovered if the correct key is chosen.

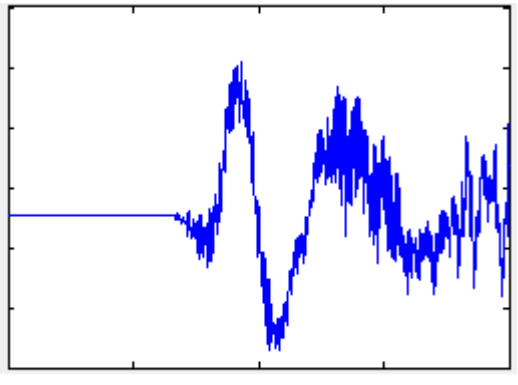
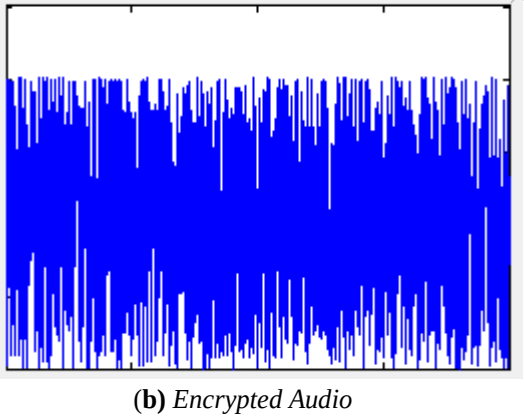
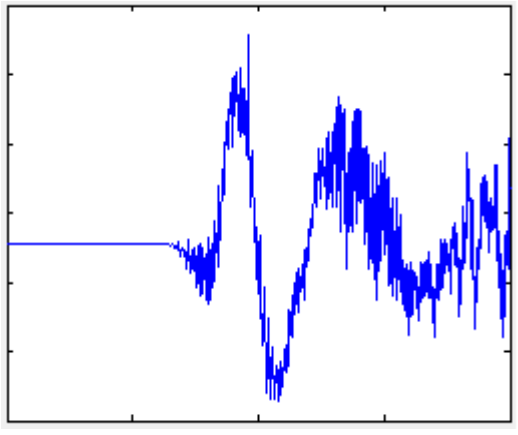


Fig 1: (a) *Original Audio*



(**b)** *Encrypted Audio*



(**c)** *Decrypted Audio*

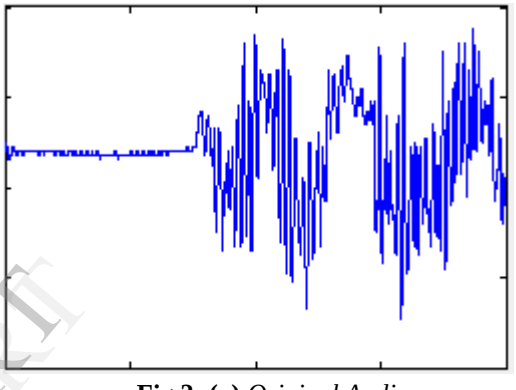
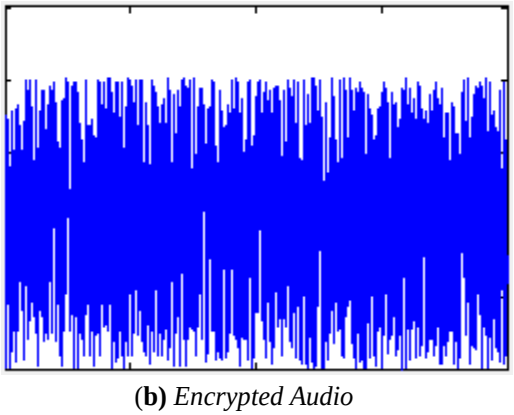
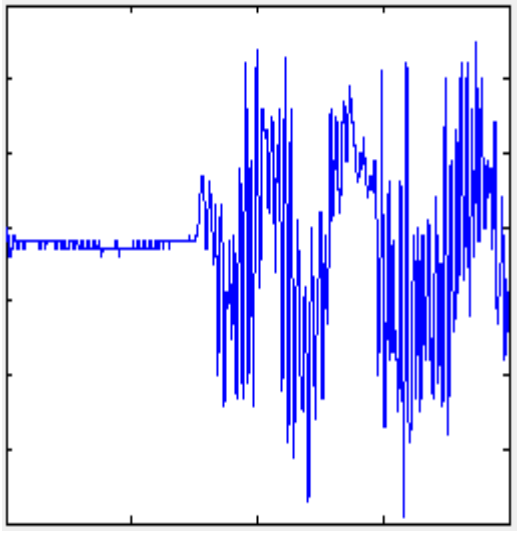


Fig 2: (a) *Original Audio*



(**b)** *Encrypted Audio*



(**c)** *Decrypted Audio*

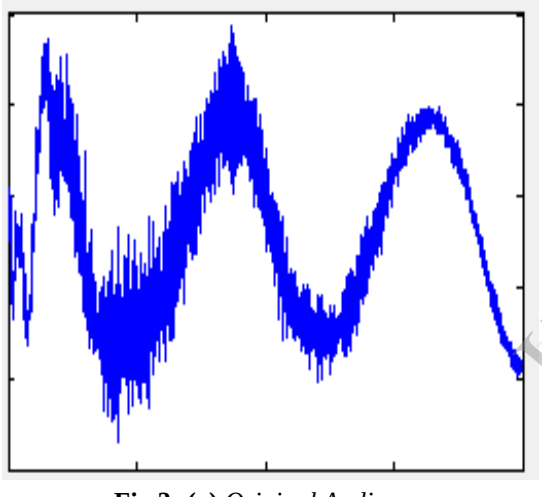
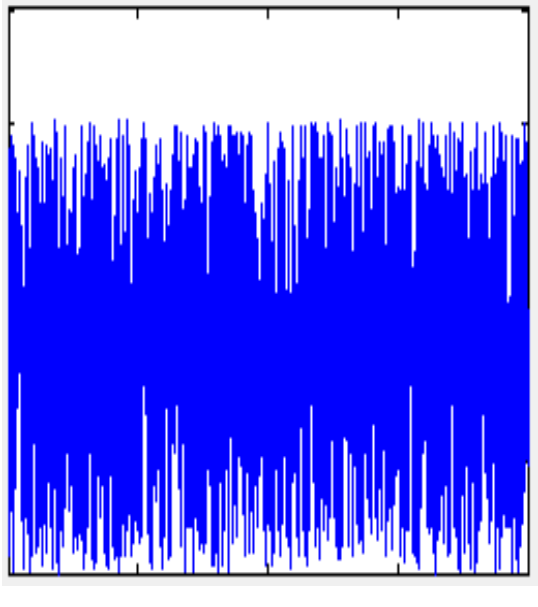
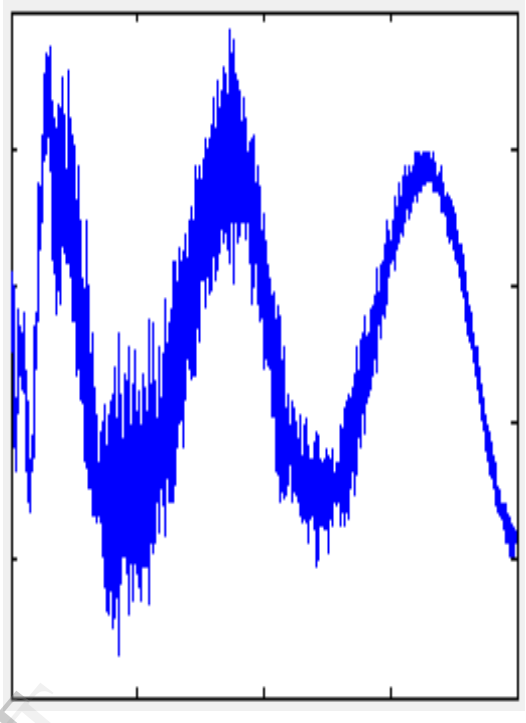


Fig 3: (a) *Original Audio*



(**b)** *Encrypted Audio*



(**c)** *Decrypted Audio*

VI. DISCUSSION & CONCLUSION

In this paper, an audio based Elliptic Curve Cryptosystem is implemented. Each value in the audio file is transformed into an affine point on the elliptic curve. This transformed value of the audio file is encrypted by the ECC technique. Decryption of ECC encrypted message is itself quite a formidable task, unless we have knowledge about the private key, the secret integer and the affine point.

The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are constrained. Such applications include chip cards, electronic commerce, web servers and cellular telephones. The work proposed for audio based encryption process can be easily extended to real-time video application.

REFERENCES

[1] Victor S. Miller, "Use of Elliptic Curves in Cryptography," *dvances in Cryptology: CRYPTO '85*, Lecture Notes in Computer Science, Vol. 218, Springer-Verlag, New York, 1986.,pp. 417-426.

[2] Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, Number 177, Jan. 1987, pp. 203-209.

[3] M.Prabu and Dr.R.Shanmugalakshmi, "A Comparative and Overview Analysis of Elliptic Curve Cryptography Over Finite field ," *International Conference on Information and Multimedia Technology* 2009.

[4] Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security", *IEEE Wireless Communications*, pp. 62- 67, Feb. 2006.

[5] Mohammad Ghamgosar and Farshad Akbari., "Application of ECC in Wireless Communication Security " , *Journal of Applied Mathematics*, vol. 03, no. 11, pp. 23-36, 2006.

[6] Yacine Rebahi, Jordi Jaen Pallares, Nguyen Tuan Minh, and Sven Ehlert, " Performance Analysis of Identity Management in the Session Initiation Protocol ", *IEEE standard*, pp. 711 - 717, 2008.

[7] C. 1. McIvor, M. McLoone, and 1. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(p)," *IEEE Trans. Circuits Syst.l* Reg. Papers, vol. 53, no. 9, pp. 1946-1957, Sep. 2006.

[8] Gang Chen, Guoqiang Bai, and Hongyi Chen, " A High-Performance Elliptic Curve Cryptographic Processor for General Curves Over GF(p) Based on a Systolic Arithmetic Unit" , *IEEE Trans. Circuits Syst. - 11:* Express Briefs, vol. 54, no. 5, pp. 412- 416, May. 2007.

[9] Standard specifications for public key cryptography, *IEEE standard*, pp.1363, 2000.

[10] Williams Stallings, Cryptography and Network Security, *Prentice Hall*, 4th Edition, 2006.

[11] Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines, Henry B.Potoczny, "Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks," *Internationaljournal of security and networks*, Vol. 2, No. 3/4, pp. 260- 271,2006.

[12] S. V. Sathyanarayana, M. Aswatha Kumar and K. N. Hari Bhat, " Symmetric Key Image Encryption scheme with Key sequences derived from random sequence of cyclic elliptic curve poits.," *International journal of network security*, Vol.3, No.2, PP.132-137, Sept. 2006.

[13] Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field," *International journal of network security*, Vol 12, No.12, PP.137-150, May. 2007.

[14] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol," *International journal of network security*, VolA, No.1, PP.99-106, Jan. 2007.

[15] R.V.Kurja, Kirti Joshi, N.Mohan Kumar, Kapil H Raranape, A.Ramanathan, T.N.Shorey, R.R.Simha, and V.Srinivas, "Elliptic Curves", *International Distribution by American Mathematical Society*, 2006.