MAT JOURNALS
Journal of Analog and Digital Communication
Volume 4 Issue 2

Design and Implementation of Video using Elliptical Curve Cryptography

Akhila A[1], Anisha Shenoy G[1], Nidhi A J[1], Preethi R[1*], Dr. A R Aswatha[2]
Student[1], Associate Professor[2]
Department of Telecommunication, Dayananda Sagar College of Engineering
Bangalore, Karnataka, India
Email: *rpreethi905@gmail.com
DOI: http://doi.org/10.5281/zenodo.2668895

Abstract

Video encryption is gaining popularity in the recent times because of growing demands of communication over the internet. The video information has to pass to and fro through several transmissions between different senders and receivers. The existing cryptographic techniques involve a complex signal processing algorithm which utilize high bandwidth and requires high processing time. Elliptical Curve Cryptography (ECC) is an algorithm that provides security with reduced processing time because of its small key size. The implementation of this video encryption algorithm has been made in Python 2.7 version. The paper gives the basic understanding of ECC followed by methodology of implementation and shows the result of encryption and decryption of the sample video.

Keywords: *Elliptical Curve Cryptography (ECC); video encryption; video decryption*

INTRODUCTION

There are numerous alternatives and approaches to video encryption. The methods like Symmetric ciphers make use of a single key for encryption as well as decryption of the video file by breaking them into different set of frames, applying the algorithm to each frame, combining the result of each and agglomerating them into a single encrypted video file. While asymmetric algorithms make use of two different keys, one for encryption and the other for decryption. The encryption process makes use of one key whereas the decryption process makes use of a different key. The existing techniques such as symmetric ciphers provide simplicity in design at the cost of security whereas asymmetric ciphers provide a better security at the cost of time. The motivation for this paper is the fact that we need to construct a certain encryption technique which could provide better security at the cost of very little time, also reducing the complexity of the design to a great extent. Thus the proposed cryptography comprises of asymmetric cipher model, Elliptical curve cryptography(ECC)[1].

The algorithm works on mp4 video format. It is commonly known as MPEG-4 part 14 or MPEG_4 AVC (Advanced Video Coding) , is a multimedia file format used to digitally store audio and video files. MP4 file format is also used for video streaming over the Internet. It is basically a container that comprises of audio and video files that are encoded digitally. More detailed understanding of ECC and video encryption is explained in the following part of the paper.

A.Elliptical Curve Cryptography

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are

also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization.

The use of elliptic curves in public key cryptography was proposed by Koblitz and Miller independently in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. A general elliptic curve takes the general form as:

$y^2 = ax^3 + bx^2 + cx + d$

Where x, y are elements of GF (p) and a, b are integer modulo p, which satisfies

$y^2 = x^3 + ax + b$ (1)

$4a^3 + 27b^2 \neq 0 \pmod p$ (2)

Point addition and point doubling are basic EC operations. Simple multiplication cannot be found in the case of elliptic curves. Suppose a single point A(x,y) on the elliptic curve can yield a resultant point B(x',y') by following a series of point addition and point doubling instead of directly multiplying the point A with a scalar, hence A=zB , where z is a scalar multiple[2].

Figure 1 shows the ECC point addition where R is the result of the addition of P and Q. Whereas Figure 2 shows the ECC point doubling where the intercept in the negative axis gives the resultant double of the point y [3].

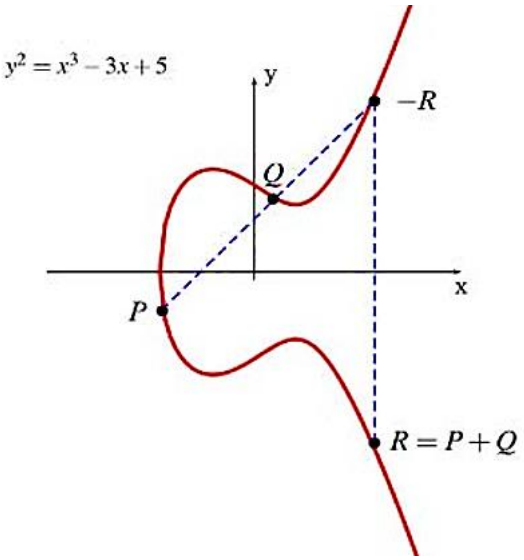

Figure 1: *ECC point doubling*

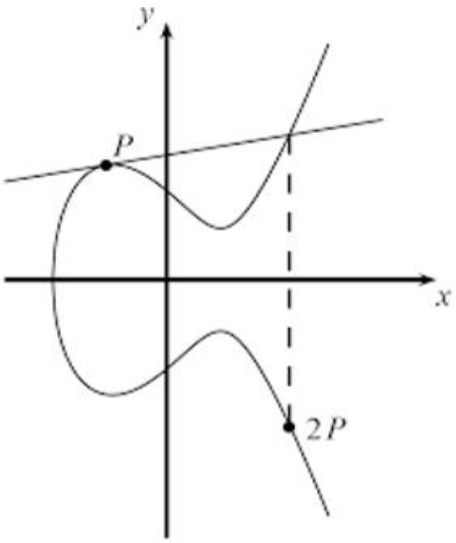

Figure 2: *ECC point multiplication*

METHODOLOGY

The proposed idea in the article is simple to understand and provides secure encryption. All the existing systems focus on complex image processing consisting of mathematical functions to provide security to the videos. They lack in one or the other parameters such as security, speed, memory constraints [4]. The video encryption using Elliptical curve cryptography is implemented using Python

The overall video encryption is as follows:

1. Read an input video information from the user .
2. Generate the public keys.
3. Encrypt the data.

The architectural block diagram for the encryption process is as shown in the figure 3.

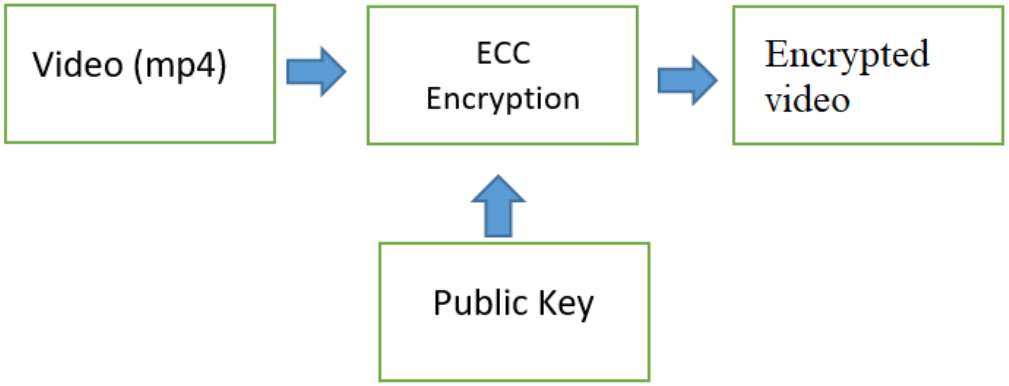

Figure 3: *Encryption process*

The overall video decryption process works as follows:

1. Receive the encrypted video content.
2. Decrypt with ECC private key to obtain the original video content.

The architectural block diagram for the decryption process is as shown in the figure 4.

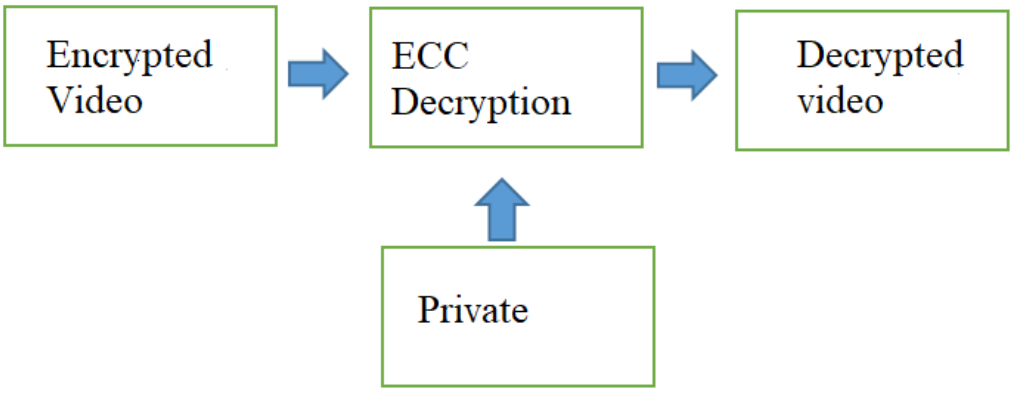

Figure 4: *Decryption process*

RESULT

Encryption and decryption of the mp4 video is done using the Elliptical curve cryptographic techniques. Figure 5 below shows the successful encryption of the sample video [5].

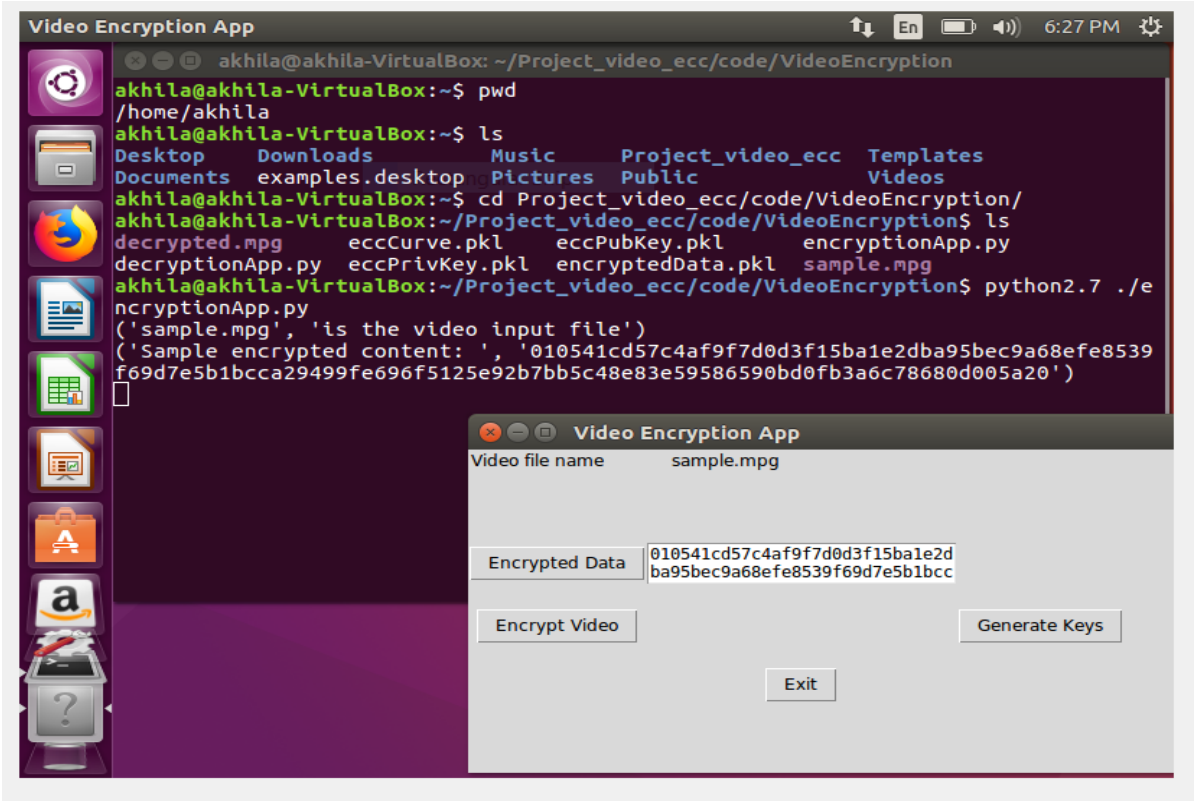

FIGURE 5: *SUCCESSFUL ENCRYPTION*

THE DECRYPTION OF THE ENCRYPTED DATA IS DONE SUCCESSFULLY. THE FIGURE 6 BELOW SHOWS THE SUCCESSFUL DECRYPTION PROCESS

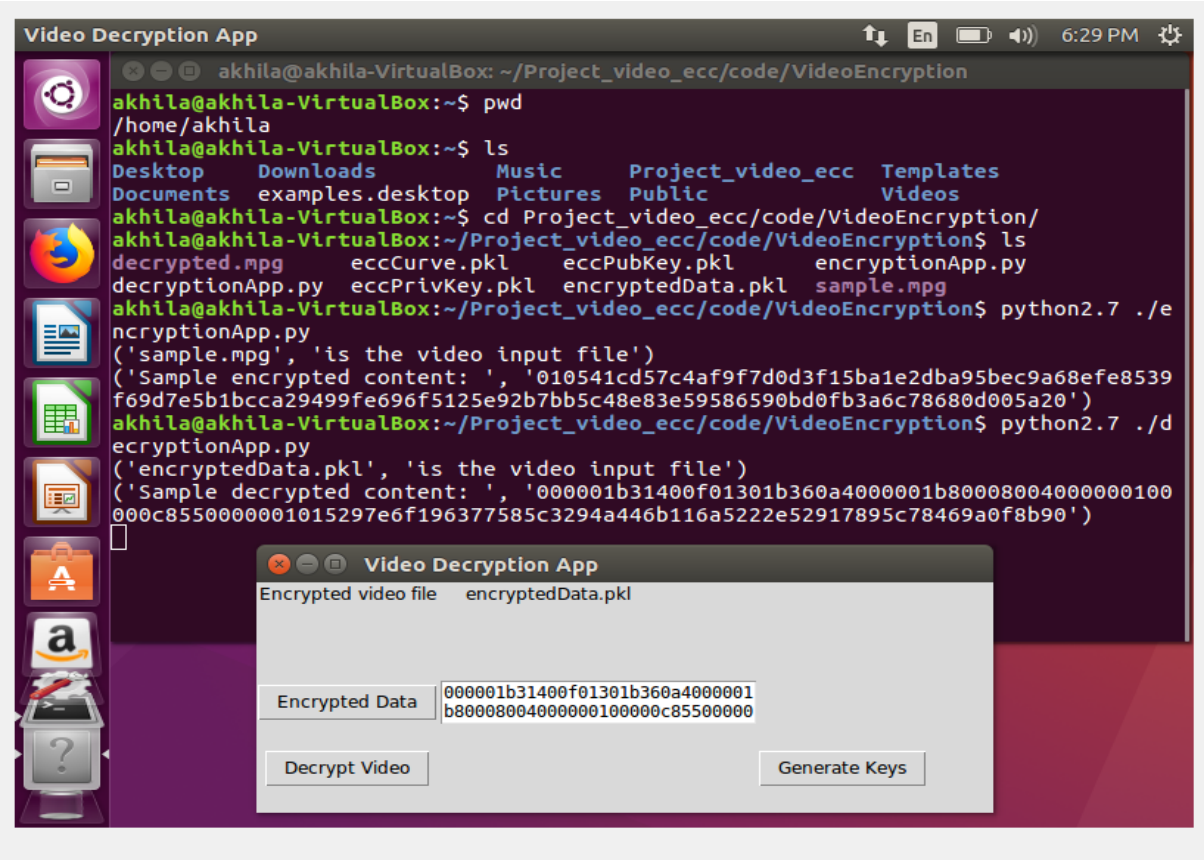

FIGURE 6: *SUCCESSFUL DECRYPTION*

CONCLUSION

The proposed algorithm and the results show us that the idea yields better results as compared to the existing techniques of video encryption. This technique is implemented in python and execution time is less compared to existing techniques. The experimental results proven in this technique has given better security compared to existing methods.

REFERENCES

1. S. C. Iyer, R. R. Sedamkar and S. Gupta, "A novel idea of video encryption using hybrid cryptographic techniques," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, 2016, pp. 1-5. doi: 10.1109/INVENTIVE.2016.7830094
2. Saied Bakhtiari, Subariah Ibrahim, Mazleena Salleh, Majid Bakhtiari, "JPEG Image encryption with Elliptical Curve Cryptography", International Symposium on Biometrics and Security Technologies(ISBAST),IEEE, 2014.
3. D,Hakerson, S.Vanstone, and A.J Menezes, "Guide to Elliptic Curve Cryptography " , 2004.
4. Dr.ParmaNand Astya1, Ms. Bhairvee Singh2, Mr. Divyanshu Chauhan3, "Image Encryption and Decryption Using Elliptic Curve Cryptography", proceedings oN IJARSE, Vol. No.3, Issue No.10, October 2014.
5. N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, VolA8, 1987, pp. 203-209.
   I. S. Reed and G. Solomon. Polynomial codes over certain finite fields.Journal of the Society for Industrial and Applied Mathematics 8:300-304,1960.

Cite this article as:
Akhila A, Anisha Shenoy G, Nidhi A J, Preethi R, & Dr.A R Aswatha. (2019). Design and Implementation of Video using Elliptical Curve Cryptography. Analog and Digital Communication, 4(2), 6–10. http://doi.org/10.5281/zenodo.2668895