Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN: 2521-3520 (online)
Volume 29, Issue 2, 2018
DOI: http://doi.org/10.23851/mjs.v29i2.438

Research Article **Open Access**

Elliptic Curve Video Encryption in Mobile Phone Based on Multi-Keys and Chaotic Map

Aya K. Naji*, Saad N. AlSaad
Department of Computer Science, College of Science, Mustansiriyah University, IRAQ.
**Correspondent author email: ayaayak9@gmail.com*

ArticleInfo

Submitted
15/01/2018

Accepted
09/02/2018

Abstract
The security of video applications in mobile devices has become recently an important field research. Dealing with video data, which is large compared to text and image and processing it in the mobile platform is a big challenge. Generally, the efficiency of any video encryption algorithm is concerned with two criteria, the computational time required to process video data, and the memory usage according to the resources on the smartphone. The secured system in 3G devices has become a matter of importance. This paper presents an implementation of full video encryption using Elliptic Curve Cryptography (ECC) on a mobile device. The operations on ECC include doubling and addition on the finite field as the backbone for an elliptic curve. Also, mapping representation is introduced to convert every byte of plain video into a point on EC. The paper proposed multi-keys instead of using one key as usual. Also, Chaotic Key Generator (CKG) is exploited for the randomness of the multi-keys. The proposed work focuses on increasing the security with multi-keys and to get acceptable time for encryption and decryption in a limited environment like mobile. The system is implemented using Android Studio with version (3.0) and using java language, it is implemented on Android version 7.0 (Nougat) and on mobile Galaxy S8.

Keywords: Video, Mobile devices, ECC, Chaotic Key Generator, Multi keys, Android OS.

الخلاصة
أصبح أمن تطبيقات الفيديو في الأجهزة النقالة في الآونة الأخيرة بحثا ميدانيا هاما. ان التعامل مع بيانات الفيديو كبير جدا اذا ما تمت مقارنتها بالتعامل مع النص والصورة ومعالجته في منصة متنقلة هو تحدي كبير. إن كفاءة أي خوارزمية تشفير للفيديو معنية بمعيارين: الوقت الحسابي اللازم لمعالجة بيانات الفيديو، واستخدام الذاكرة وفقا لموارد الهاتف الذكي. أصبح النظام الحماية في أجهزة الجيل الثالث 3G مسألة ذات أهمية. يقدم هذا البحث إجراء تشفير الفيديو بصورة كاملة باستخدام تشفير المنحني الاهليلجي (ECC) على جهاز نقال. تشمل عمليات (ECC) المضاعفة والاضافة على حقل محدود باعتبارها العمود الفقري لمنحني الاهليلجي. كما يتم عرض تمثيل الجدول لتحويل كل بايت من الفيديو العادي إلى نقطة على EC . اقترح هذا البحث استخدام مفاتيح متعددة بدلا من مفتاح واحد كالمعتاد. يتم أيضا استغلال Chaotic Key Generator (CKG) لعشوائية المفاتيح المتعددة. ويركز العمل المقترح على زيادة الأمن مع مفاتيح متعددة والحصول على وقت مقبول للتشفير وفك التشفير في بيئة محدودة مثل المحمول. يتم تنفيذ النظام باستخدام نظام اندرويد ستوديو Android Studio بالإصدار (3.0) واستخدام لغة الجافا، تم تنفيذها على نظام اندرويد الإصدار 7.0 (Nougat) وعلى الجهاز النقال Galaxy S8.

Introduction

Multimedia information like graphics, images, audio, and video have been widely used in a smartphone device. Protection in video conference, video surveillance, pay-TV, etc. becomes a challenging work in video communication especially for the wireless mobile device [1].

Cryptography is the transformation of a plain message to unreadable form to be secure and immune from intruders. Information security algorithms are widely used in the recent times to protect data [2]. Symmetric encryption schemes are utilized a single key for both encryption and decryption such as (DES, RC4, AES,..., etc.). Asymmetric encryption schemes are used two keys, the message to be encrypted is encrypted with the public key of the receiver. The receiver can then reverse the encryption

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.

using the private key associated with the public key, such as (RSA, ECC,..etc.) [3].

ECC is Asymmetric key cryptography that requires a public key and a private key [2]. ECC can be a good candidate in many new fields need security requirements, particularly in embedded systems, for example, cell phones [4].

ECC is one of the most effective systems that are used for secure and immune from impostors. This is because it is hard for the opponent to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) [5]. ECC would have main advantages over a classical system such as speed increasing, short memory, and also smaller key size. It can be said that the memory and the power are low. Also, the storage is less than other systems, that motivate to use security on some specific platform like wireless-devices and laptop. [6]. ECC encryption process and decryption process cannot encrypt and decrypt real plain text, they just can encode and decode points on the curve. Therefore, the encoding means altering a plain text character into points defined by the EC in order that to be appropriate to encrypt, however, decoding means changing the points in the original character [7].

There are several public key cryptosystems based on the ECDLP such as elliptic curves Diffie-Hellman key exchange, elliptic curves Massey-Omura, Menezes-Vanstone elliptic curve cryptosystem, and elliptic curves ElGamal public key cryptosystem. Table1 illustrates some algorithms that can be exploited for the type of application.

Literature Review

K. Rahouma, proposed multi-curve on ECC algorithm to encrypt files with additional parameter rather than one curve, the message is divided into blocks such at each block is of length less than the smallest prime number of the used ECC, each block has a private key and changes from one block to another [8].

D. S. Kumar, CH. Suneetha A.Chandrasekh AR, proposed two special equations on ECC algorithm to use for encryption rather than one as in stander ECC, these equations used addition and doubling operations, they also added another parameters, and utilized private key for each character in the message [9].R. Singh, R.Chauhan, V.K. Gunjan, P.Singh, present ECC over finite field with prime number p>3, they have converted a character to the point according to Koblitz equation to encrypt audio [10].

Table 1: Application for Public-Key Cryptosystem

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie -Hellman	No	No	Yes
DSS	No	Yes	No

M. Naik, A. Sindkar, P. Benali, C. Moralwar, present an algorithm that combine AES and ECC to encryption files under mobile platform (Android SO) [11]. D. M. Dumbere, N. J. Janwe, used AES algorithm to encrypt video, they have compared with DES algorithm [12]. A. Tariq, F. Hadi, add some a modifications on the classical AES to increase security, and implementation is on any file of data under the mobile platform (Android OS) [13]**.** Also, A. Kareem, implement two types of modifying on AES to encrypt video under windows platform [14].

Materials and Methodologies

Mathematics preliminaries

Some of the mathematical operation that we will be using while performing the implementation of the video encryption/decryption using ECC. ECC used Group and Field [15]. Field accomplish the usual arithmetic properties [16].

- Prime field F_p where p is a prime.
- Binary field F_2^m where m is a positive integer.

Elliptic Curves over Prime Curve

Let F_p be a finite field and p is prime which is called Galois Field (GF). The elliptic curve is a curve consists of points satisfies the equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \qquad (1)$$

When x, y, a, and b are elements in GF(p). a and b parameters should be satisfied to the condition:

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

The EC over prime curve GF(p) is called non-singular curve when the above condition equ.2 satisfies, otherwise, it is called (Singular elliptic curve) [17] [4].

It is noticed to realize that the number of points in a finite abelian group defined over an EC. The number of points #E is bounded by Hasse's theorem in the case of the finite groupE_p(a,b) [4]:

Table 2: An abstracted features for related work.

Related Work	Platform		Algorithm	Cryptography		Data	Programming Language
	Computer Platfrom (Windows)	Mobile Platform		Symmetic	Asymmetric		
1	-	-	ECC propsal		☑	Not - determined	It did not specify - the language program
2	-	-	ECC propsal		☑	Not - determined	It did not specify - the language program
3	-	-	ECC		☑	Sound	It did not specify - the language program
4		☑	AES & ECC	☑	☑	Not - determined	Android Studio
5	☑		AES	☑		Video	Matlab
6		☑	AES propsal	☑		Text,Image,Sound,Video,and any file	Android Studio
7	☑		AES propsal	☑		Video	C#

Hasse's theorem

Given an elliptic curve E modulo p, the number of points on the curve is denoted by #E and is bounded by p+1-2$\sqrt{p} \leq$ #E $\leq$ p + 1 + 2$\sqrt{p}$ Hasse's theorem (or Hasse's bound) states that the number of points is about in the scope of the prime p [4].

Mathematical for ECC

1. Point Addition
   P (x_p, y_p) and Q (x_Q, y_Q) are points, with P ≠ Q, then R = P + Q = (x_R, y_R) is determined by the following rules:

$$x_R = (Slope^2 (x_p - x_R) - y_p) \bmod p \quad (3)$$

$$y_R = (\text{Slope} - x_R - x_Q) \bmod p \quad (4)$$

Where

$$Slope = \frac{y_Q - y_P}{x_Q - x_p} \bmod p \quad (5)$$

2. Point doubling

P(x_p, y_p) and Q(x_Q, y_Q) with P ≠ Q, then R = P + Q = (x_R, y_R) is determined by the following rules in Equation 3 and 4:
Where

$$Slope = \frac{(3x_1^2 + a)}{2y_1} \; mod \; p \quad (6)$$

3. Point subtraction
   P (x_p,y_p) - Q(x_Q, y_Q) = P (x_p, y_p)+ Q (x_Q, $-y_Q$)
4. Point multiplication is defined as repeated addition; for example, 4P = P + P + P + P.

ElGamal Cryptosystem

The EC ElGamal protocol can be a very useful protocol for key exchange, digital signature and message encryption [18]. Consider Alice and Bob are the two communicating parties. They agree upon a common elliptic curve equation (1) and a base point B. Let Alice and Bob private keys be d and e respectively. Alice and Bob public keys are given by Q_A= e.B and Q_B=d.B respectively. If Alice want to send a message 'Pm' to Bob, Alice uses Bob's public key to encrypt the message. Encryption side equation is $C_m = [(e.B); (P_M + e.Q_B)]$ and decryption side equation is $P_m = [C_m - d.(Q_A)]$ [2]. The original algorithm uses one key and our algorithm uses multi-keys instead of one key.

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.

Proposed System Multi keys Elliptic Curve Cryptography Encryption and Decryption on ElGamal

The proposed system is depicted in Figure1. The figure illustrates that there are two parts encryption side and decryption side. The encryption side consists of the stages: (Chaotic Key Generator (CKG), ECC Operations, Build Multi Keys and Encryption).The decryption side consists of: (Chaotic Key Generator, ECC Operations, Build Multi Keys and Decryption). Each stage of the proposed system is described in details, with their needed representation, figures and also algorithms.

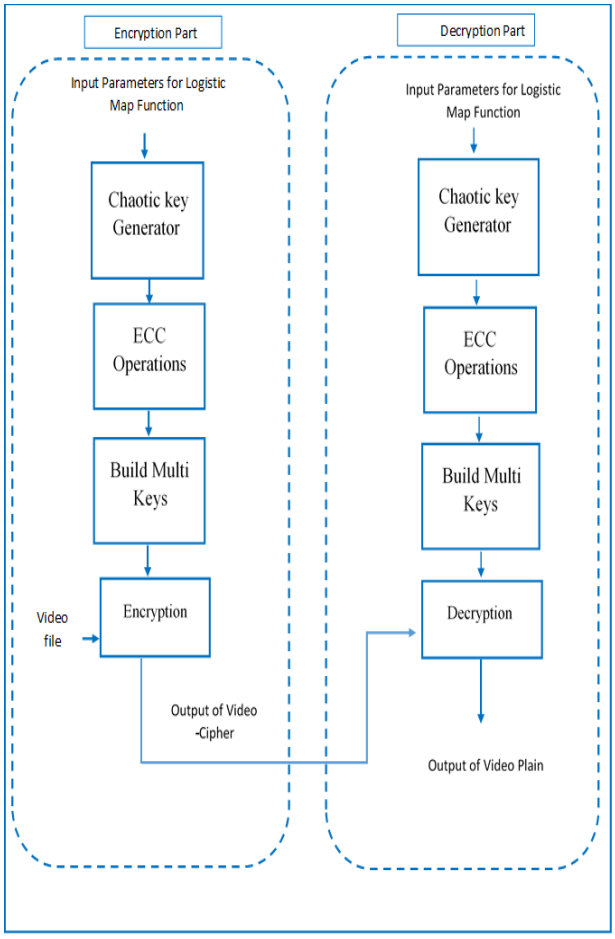

Figure 1: The Block Diagram of System.

A. Encryption part

The task of this part is to encrypt video file in mobile.

STAGE 1 Chaotic Key Generator (CKG)

A chaotic system is a nonlinear deterministic dynamical system which exhibits random behavior. The logistic map function is indicated as:

$$x_{n+1} = r.x_n.(1 - x_n) \quad (7)$$

The above function is implemented to generate two types of keys: key1 and key2 with 256 lengths each this function is used to exploit the behavior of high randomness and sensitivity, the following algorithm describes logistic map function.

Algorithm 1: Logistic Map Function.

Input
x: An array of 256 cells
index key =256
Output
Chaotic // array of chaotic random numbers.
Begin
Step1
Set $x_{(0)}$ // value $0 \leq x_{(0)} \leq 1$; key1
Set $r_{(0)}$ // value $3.6 \leq r_{(0)} \leq 4$; key2
Step2
For n ← 0 **to** index key **Do**
$x_{(n+1)} \leftarrow r^* x_{(n)}{}^*(1 - x_{(n)})$ //Perform the equ.(7)
End For
Step3
Sort x_n in descending
Step4
Chaotic ← x_n //put the values after sort in matrix of chaotic
End for
End

The output from of the stage is an array of 256 chaotic values as shown in the Table 3. The first column represents the index storing of results. The second column represents the results before sorting. The third column represents the index storing of results after descending order. The fourth column represents the results after descending order.

STAGE 2 ECC Operations

This represents the second stage in encryption part. The stage itself consists of process four processes: Domain Generator, Inverse Finding, (Addition, Doubling, and Multiplication) are explained previously.

Generate Domain the aim of this process to build curve over finite field F*q* of prime and to generate the domain according to parameters

$E_p(a,b)$, the implementation is illustrated in algorithm in [19].

Table 3 Logistic map function before and after sort

indx Before Sort	LMF Before Sort	indx After Sort	LMF After Sort
0	0.65193513	33	0.917465163
1	0.832780679	175	0.917221046
2	0.511073263	21	0.917180745
3	0.917049995	187	0.917082539
4	0.279174337	3	0.917049995
5	0.738536217	99	0.916882662
6	0.708678736	79	0.916869254
7	0.75768319	239	0.9167824
8	0.673809702	167	0.915896329
9	0.806629989	123	0.915545352
10	0.572439444	151	0.915026203
.		.	
.		.	
.		.	
253	0.937203694	178	0.219790282
254	0.220698487	142	0.219727593
255	0.644964993	29	0.219726617

Figure 2 shown the output from this process are group of points over $E_{751}(-1,188)$, number of points generated are 726 points {(0,375), (0,376), (1,375), …, (750,376)}.

STAGE 3 Build Multi Keys

The aims of this stage are built 256 keys used for encryption and decryption. It is worthy to mention that step 2 of the algorithm (5.2) requires performing the: doubling, addition, and multiplication these operations are explained in section 4.1. Also step 2 requires finding the inverse use extended Euclidean algorithm. Algorithms (5.2) illustrates the main abstracted steps to generate 256 keys and Figure 3 shows two sets of keys that used for encryption and decryption.

Algorithm(5.2)Build multi-keys

Input

Select 256 keys from the number of order #E

B is base point

Output

$e = [e_0, e_1, e_2, \dots, e_{255}]$

// Private keys as an array of side encryption (Alice keys).

$d = [d_0, d_1, d_2, \dots, d_{255}]$

// Private keys as array of side decryption (Bob keys).

$Q_B = [Q_{B0}, Q_{B1}, Q_{B2}, \dots, Q_{B255}]$

// Public keys as array of side decryption (Bob public keys as points).

$e_{new} = [e_0, e_1, e_2, \dots, e_{255}]$

//New array of side encryption (Alice keys) after arranging according to CKG.

$d_{new} = [d_0, d_1, d_2, \dots, d_{255}]$

//New array of side encryption (Bob keys) after arranging according to CKG.

$Q_{B\,new}\ [Q_{B0}, Q_{B1}, Q_{B2}, \dots, Q_{B255}]$

// New array of public keys for side decryption (Bob public keys)

Begin

Step1

Generate two arrays of 256 random keys for two side encryption and decryption denote e and d, the range of keys between $1 \le key \le \#E$ and multiple keys must not be duplicated.

Step2

Calculate public keys for side decryption

$Q_B = B \cdot d$

Step3

Permutation (e, d, and Q_B) according to CKG algorithm (5.1) to get (e_{new}, d_{new} and $Q_{B\,new}$).

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.

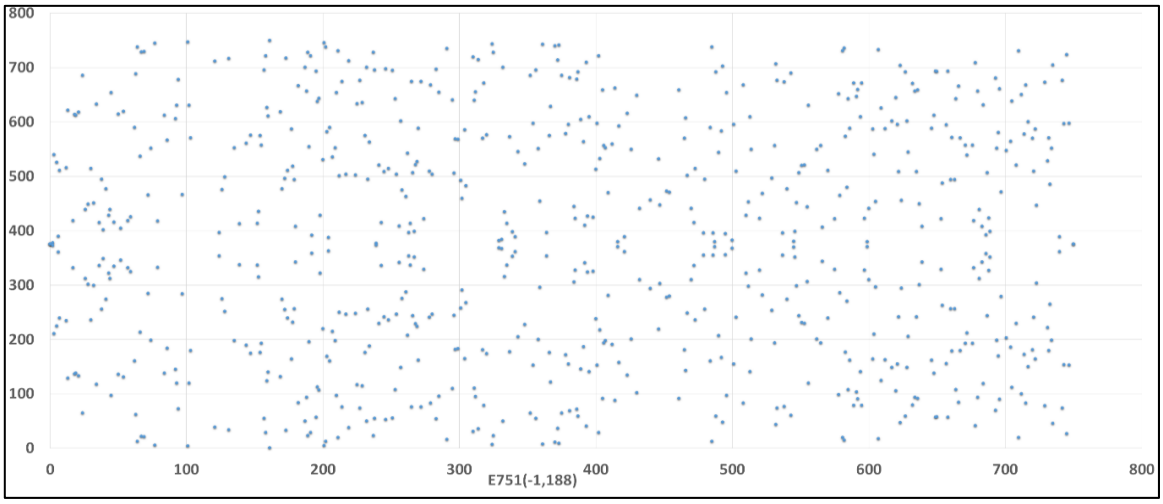

Figure 2: Generate domain process

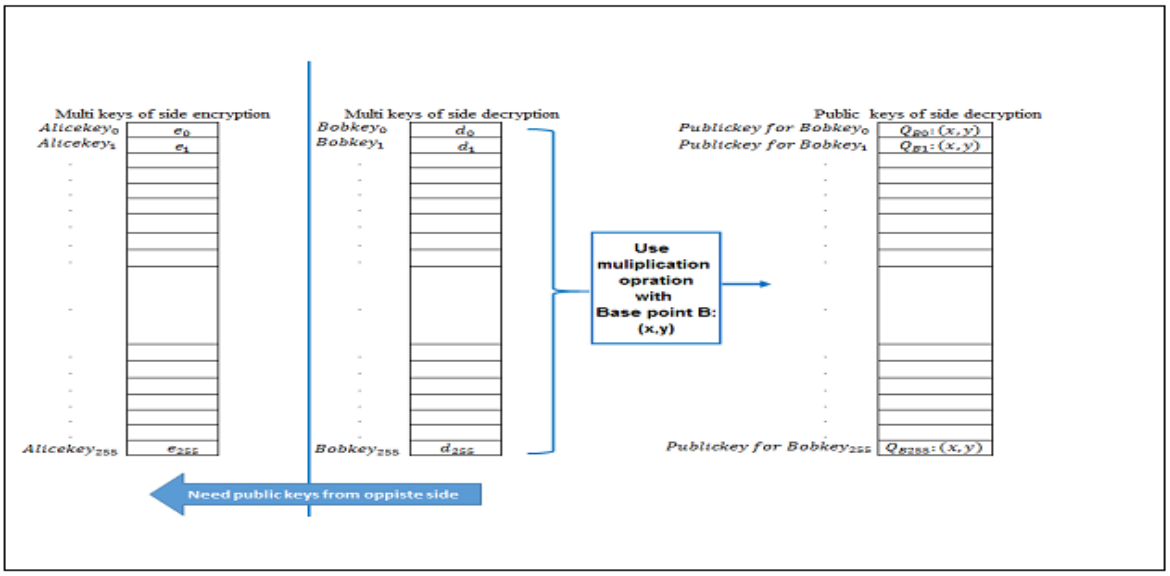

Figure 3: Building Multi keys For Side Encryption

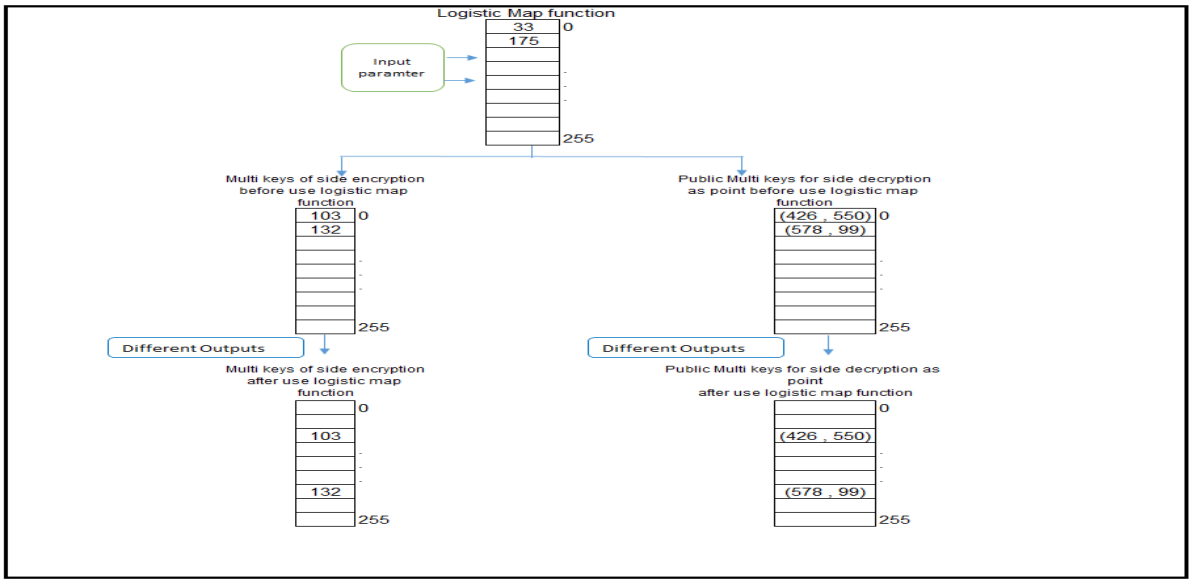

Figure 4: The structure of matrixes for multi-keys according to logistic map function in the system

STAGE 4 Encryption

This stage may be the core of the encryption part. It is task is to encrypt video file stored in mobile with full encryption, the implementation is illustrated in the Algorithm (5.3).

Algorithm(5.3): Encryption of the ElGamal Proposed

Input

B // Basepoint

e_{new} // The result is an array of several keys from an algorithm (5.2).

d_{new}// The result is an array of several keys from an algorithm (5.2).

Q_{new}// The result is an array of several public keys from an algorithm (5.2).

P_m // Video plain text

Output

C_m// Encrypted video

Q_A// The result from e B represents public keys for side encryption

Begin

For P_m = o **To** length of video **Do**

Begin

Step1

Generate 256 encryption points from below equation:

$C_{m0} = [(e_0 B); (P_{M0} + e_0 Q_{B\ new\ 0})]$

$C_{m1} = [(e_1 B); (P_{M1} + e_1 Q_{B\ new\ 1})]$

$C_{m2} = [(e_2 B); (P_{M2} + e_2 Q_{B\ new\ 2})]$.

$C_{m255} = [(e_{255} B), (P_{M255} + e_{255} Q_{B\ new\ 255})]$

Step2

Represent these points according to ASCII code.

End

End

Step3 Output video ciphertext.

A. Decryption part

The task of this part is to decrypt a mobile video cipher, the first stages (Chaotic Key Generator (CKG), ECC operations, and Build multi-keys) are similar in processing as encryption part but the output is slightly different.

STAGE 1 Chaotic Key Generator (CKG) same process in encryption side.

STAGE 2 ECC Operation same process in encryption side.

STAGE 3 Build Multi keys

Which was explained in building multi-keys of part encryption with some difference. The Figure 5 as shown below and call build multi-keys algorithm (5.2).

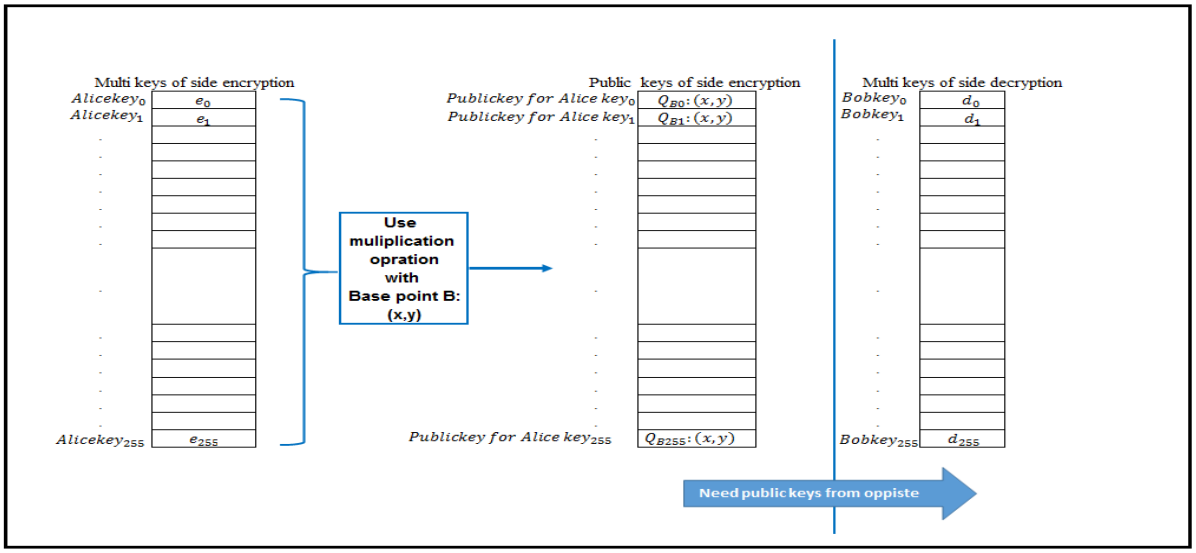

Figure 5: Building Multi keys For Side Decryption

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.

STAGE 4 Decryption

This stage may be the core of the decryption part. It is task is to decrypt video file stored in mobile with full encryption, the implementation is illustrated in the Algorithm (5.4)

Algorithm(5.4)Decryption of The ElGamal Proposed

Input

d_{new} // The result is an array of several keys from an algorithm (5.2).

Q_A // The result is an array of several public keys of side encryption from an algorithm (5.2).

C_m //Video cipher text

Output Video plain text

Begin

For C_m = 0 **To** length of video **Do**

Begin

Step1 Generate 256 decryption points from below equation:

$P_{m0} = [C_{m0} - d_{new\,0}(Q_{A0})]$

$P_{m1} = [C_{m1} - d_{new\,1}(Q_{A1})]$

$P_{m2} = [C_{m2} - dnew_{\,2}(Q_{A2})]$

.

.

.

$P_{m255} = [C_{m255} - d_{new\,255}(Q_{A255})]$

Step2

Represent these points according to ASCII code

End

End

Step3 Output video plain text.

Results and Discussion

The mobile applied in the encryption and decryption of the video process is (Galaxy S 8) has hardware (RAM 4GB, internal storage 64 GB) and has software (Android 7.0 (Nougat)). This system depends on well-known video format extension of MP4. Table 4 presents the video files and the time required for encryption and decryption.

Also, the curve for each file is depicted for encryption and decryption comparing with the size of the file in Figure 6 and Figure 7 respectively.

Table 4 Time Execution

File name	Video sample	Size of Video	Time Encryption MM:SS	Time Decryption MM:SS
Va		0.91 MB	00:11	00:13
Vb		1.15 MB	00:14	00:17
Vc		1.92 MB	00:25	00:28
Vd		2.28 MB	00:28	00:33
Ve		2.46 MB	00:31	00:37
Vf		2.54 MB	00:31	00:38
Vg		2.56 MB	00:31	00:37
Vh		4.97 MB	01:01	1:11
Vi		5.00 MB	01.02	01:22
Vg		5.29 MB	01:08	01:19
Vk		6.61 MB	01:24	01:38
Vl		6.89 MB	01:26	01:40
Vm		10.1 MB	02:08	02:30
Vn		13.6 MB	02:54	03:24

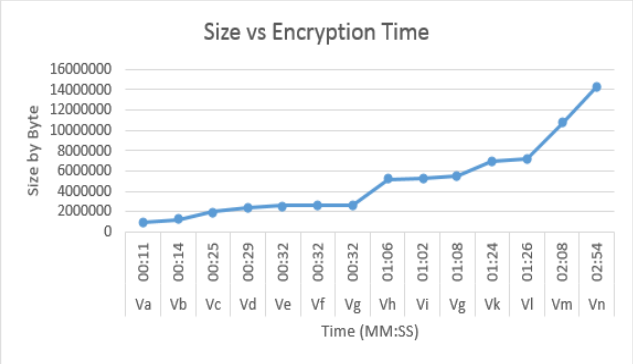

Figure 6: Encryption Time for ECC

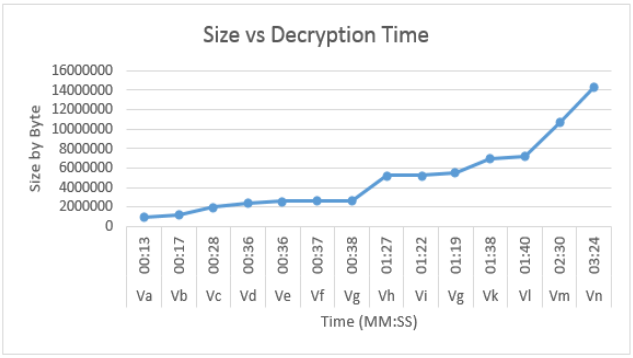

Figure 7: Decryption Time for ECC

After we use the side encryption algorithm ECC of operation to access program and get

the video file from the video store, we will notice the video as shown in Figure 8.

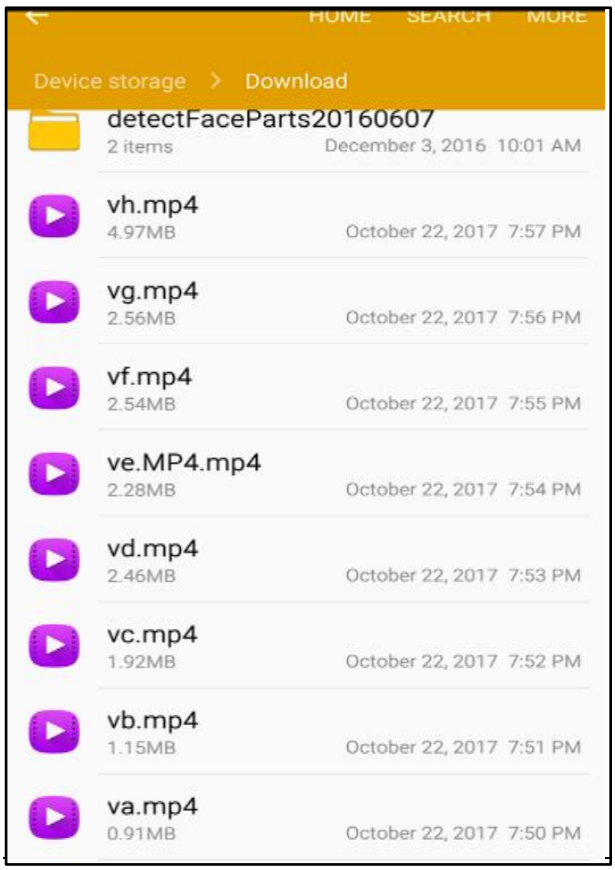

Figure 8: Video encryption

When we click on any video encryption does not display video and show the message as shown in Figure 9.

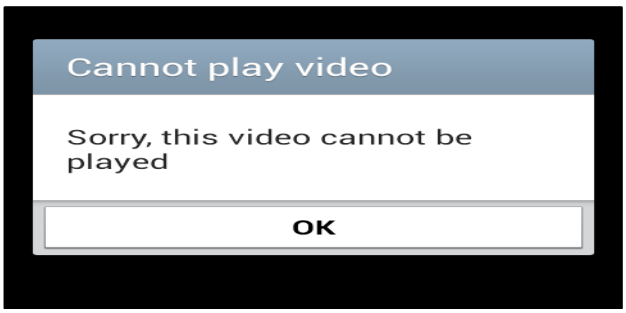

Figure 9: Video message

When we use the side decryption algorithm ECC of operation to access program and get the video decryption file from the video store, we will notice the video as shown in Figure 10.

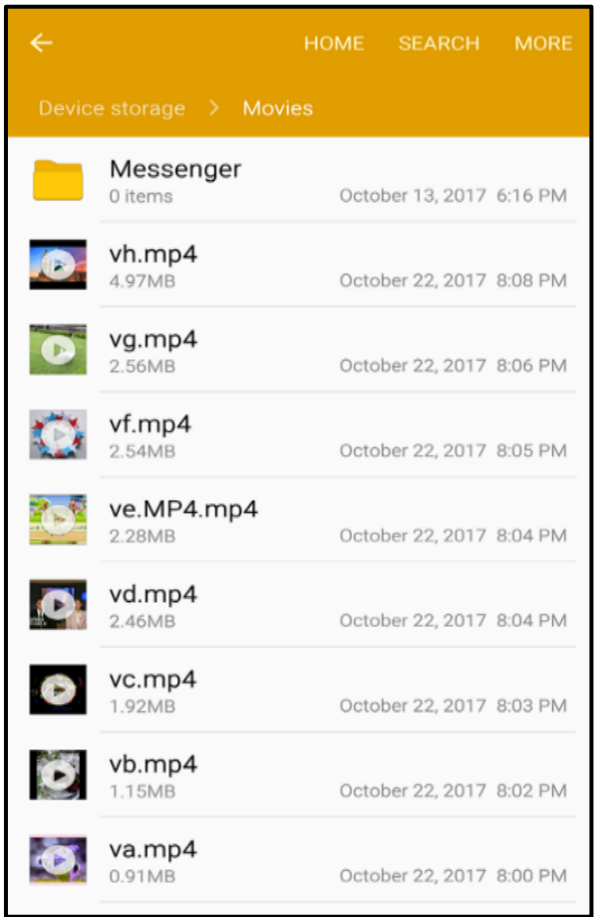

Figure 10: Video Decryption.

Conclusions

The application has achieved the protection for video of data in mobile devices by using full encryption. It can be used for all types of media like text, image, and sound. It is noted that the decryptions take a little more time relatively with the encryption time required and this is acceptable because of the nature of the algorithm besides that the algorithm is implemented in limited resources memory in the mobile platform compared with the computer platform. The application is easy to use. It needs only two keys to implement. The result depends on the specification, of the mobile and kind of OS, thus the results are different according to the type of both phones and OS used.

For the future work, using ECC in a different environment, such as applying it to iPhone. It can be used as an online application using an algorithm to exchange keys between the users and connect the application to a storage

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.

website for key exchange. Searching the use of multiple keys in another domain and apply them in other algorithms to their limitations in current researchers. Build multi-keys with different domain of $E_p(a, b)$ and select the multi keys as randomly under control of user. The use of algorithm Menezes-Vanstone ECC in the mobile with the addition of a proposed by dividing the file into two parts, one for the odd bytes and the even bytes and applied the equations ones for odd bytes and second for even bytes

References

[1] P.Saranya, L.M.Varalakshmi, " H.264 based Selective Video Encryption for Mobile Application" *International Journal of Computer Applications,* vol. Volume 17– No.4, pp. 21-25, 2011.

[2] L.D.Singh, K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography" in *Eleventh International Multi-Conference on Information Processing*, Elsevier, 2015.

[3] "Technical Guideline – Cryptographic Algorithms and Key Lengths" Federal Office for Information Security, Germany, 2017.

[4]C.Paar,J.Pelzl,"Understanding Cryptography A Textbook for Students and Practitioners" Springer, 2010.

[5] Z. E. Dawahdeh, S. N. Yaakob, R. R. B. Othman, "A New Modification for Menezes-Vanstone Elliptic Curve Cryptosystem," *Journal of Theoretical and Applied Information Technology,* vol. 85, no. 3, pp. 290-297, March 2016.

[6] P. S. Yadav, P. Sharma, K. P. Yadav, "Implementation of RSA Algorithm Using Elliptic Curve Algorithm for Security and Performance Enhancement," *International Journal of Scientific & Technology Research,* vol. 1, no. 4, pp. 102-105, May 2012 ISSN 2277-8616.

[7] L. Tawalbeh, M. Mowafi, W. Aljoby, "Use of Elliptic Curve Cryptography for Multimedia Encryption," *IET Information Security,* pp. 1-8, 2012.

[8] K. Rahouma, "A Modified Menezes-Vanstone Elliptic Curve Multi-Keys Cryptosystem,"www.semanticscholar.org , Riyadh, Kingdom of Saudi Arabia, 2006 .[Online].Available: https://pdfs.semanticscholar.org/d13c/05f9256790d9af7637009168b3018fdaf06b.pdf..

[9]D.S.Kumar,CH.Suneetha,A.ChandrasekhAR, "Encryption of Data Using Elliptic Curve Over Finite Fields," *International Journal of Distributed and Parallel Systems,* vol. 3, no. 1, pp. 103-108, January 2012.

[10] R. Singh, R. Chauhan, V. K. Gunjan, P. Singh, "Implementation of Elliptic Curve Cryptography for Audio Based Application," *International Journal of Engineering Research & Technology (IJERT),* vol. 3, no. 1, pp. 2210-2214, January - 2014.

[11] M. Naik, A. Sindkar, P. Benali, C. Moralwar, "Secure and Reliable Data Transfer on Android Mobiles Using AES and ECC Algorithm," *International Journal of Innovative Technology & Adaptive Management (IJITAM),* vol. 1, no. 11, 2014.

[12] D. M. Dumbere, N. J. Janwe, "Video Encryption Using AES Algorithm," in *2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14, IEEE,* Coimbatore, India, July 8, 2014.

[13] A. T. Sadiq, F. H. Faisal, "Modification AES Algorithm Based on Extended Key and Plain Text," *Journal of Advanced Computer Science and Technology Research,* vol. 5, no. 4, pp. 104-112, 2015.

[14] A. Kareem, "An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Video Applications," MSc thesis in Computer Sciences, Al-Mustansiriyah University, Iraq, 2015.

[15] S.Y.Yan, Number Theory for Computing, Springer, 2000.

[16] A. B. ÖZCAN, "Performance Analysis Of Elliptic Curve Multiplication Algorithms For Elliptic Curve Cryptography," M.Sc., Department of Electrical and Electronics Engineering ,Middle East Technical University, 2006.

[17] W.Stallings, "Cryptography and Network Security Principles and Practice ", 2011, 5th Edition.

[18] A. Malik, "Reconfigurable Elliptic Curve Cryptography," Msc, Kate Gleason College of Engineering, 2005.

[19] A.K.Naji ,S.N.Alsaad, "Data (Video) Encryption in Mobile Devices," *Kurdistan Journal for Applied Research*, vol. 2, no. 3, 2017.

Copyright © 2018 Authors and Al-Mustansiriyah Journal of Science. This work is licensed under a Creative Commons Attribution-NonCommercial 4. 0 International Licenses.