Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822p-ISSN: 2958-0862

Elliptic Curve Cryptosystem for Digital multimedia, General Review

Dina.H. Abbas[1, *], Ayad Abd-al-Kahhar AbdulSalam[1]

[1]Computer Science Department, College of Science for Women, University of Baghdad , Baghdad, Iraq

*Corresponding Author: Dina.H. Abbas

DOI: https://doi.org/10.55145/ajest.2023.02.02.008
Received January 2023; Accepted March 2023; Available online March 2023;

ABSTRACT: Various Cryptography algorithms are used to keep the transmission of data safe from intruder and to secure the connection between sender and receiver. This article provides an overview of ECC, including the algorithm process, fundamental protocols, and different ECC systems and applications. EC over fields also represents by numerous graphical representations of cryptographic processes. Comparison tables are included that list the ratio of key size between ECC and RSA (the nearest method to ECC), in factors of overhead, power availability and required storage, which indicates fast running with less bandwidth in case of elliptic curve method. In the other hand some previous works related to the topic were compared according to the functions of properties, measurement methods, and type of the data used, results were collected in traceable manner for the purpose of making it available to researchers and those interested in ECC.

Keywords: Elliptic curve, private key, public key, finite field

1. INTRODUCTION

Digital communication is growing rapidly in the recent years, most of people around the world using smartphones, Electronic currency trading, correspondence of large companies, online shopping [1], even in the field of study and education, now listening to lectures, holding conferences and seminars, all of this is done through electronic media, and communication between a web browser and a website or voice communication between individuals. All these applications are vulnerable to spy; this is leading to increase the necessity of the information security that is important for data transmission over the internet, it includes digital multimedia such as text, audio, image, and video. The key worry for data exchange between unknown parties is the crucial matter of security for Confidentiality, Integrity, and Availability (CIA)[2]. Today, the effectiveness of private communication between parties is intimately tied to the success of commercial activities. As a result, there is an increasing demand for information of digital multimedia content security to preserve secrecy and avoid fraud, this may be addressed by using cryptography. [3]. This review paper, present a detailed study on Elliptic Curve Cryptography (ECC) for digital multimedia methods to preserve security through various techniques of Elliptic curve. The review can be exactly give the main and most recent research progress of ECC method developed in the literature for solving multimedia data security and Confidentiality problems. Furthermore, view the elliptical curve protocols used to provide data protection between the parties that communicate with each other's.

2. CRYPTOGRAPHY

The study of mathematical techniques related to aspects of information security called Cryptography. CIA triad in Cryptography deals with techniques of transmitting information in a secret manner to protect the information from unauthorized parties, even if the transmission is done through an insecure channel.

The cipher process is the finished process of hiding text using a certain algorithm. The encryption process) E (hides the original message (called plaintext P) using the encryption key (K_{EN}), (and the encrypted content is termed (cipher text C). Decryption process (D) is the reverse of encryption process, and it uses the same mechanism as encryption to retain the plaintext (P) from cipher text (C) by the decryption key (K_D). Below is the equations that represent the aforesaid processes [4].

$$C\_ciphertext = EK_{EN} (P\_plaintex) \quad (1)$$

Where K_{EN} means the key for encryption

$$P\_plaintex = DK_D\ (C\_ciphertext) \quad (2)$$

Where K_D means the key for decryption

The scope of cryptography is categorized according to the kind of key that used in the cryptographic systems, symmetric key also called secret key algorithms and asymmetric key algorithms that called public key algorithms, these types are present in the next paragraphs [4], after that elliptic curve cryptography (ECC) which a kind of asymmetric-key cryptography will explain carefully[3].

2.1 Private-key cryptography

It is the oldest and fastest type of cryptography and also it's known as (Symmetric Key) Cryptography. In this type both of them (sender, receiver) agree on a common key that the sender uses in the encryption process, and the recipient uses the same key for decryption processes. Because in Symmetric Key Cryptography (sender and receiver) must share the same key in a secret manner, therefore the key management problem appears where is more difficult in a large network, this is a disadvantage of this type of cryptography that has been solved in a public key scheme. On the other hand, using the same key for both parties has benefits such as ease of implementation and speed of encryption and decryption processes[4], [5] .

2.2 Public key cryptography

The importance of asymmetric key encryption, which is also called (public key) encryption came from solving this type the problem of distributing keys that had to be sent through a secret channel between the two parties (sender and receiver) that were encountered in the previous type of encryption, and this was done using each of them with different keys form the other party, the recipient first generates private and public keys, keeps his private key for use in the decryption process while declaring the public key, when the sender wants to send a message, he uses the public key in the encryption process that was generated and announced by the recipient in advance, noting that although private and public keys were different, but in fact the public key is mathematically dependent on the private key. As such, the owner is the only one who know the private Key, while any person who wants to communicate with the owner should know the public key [3].

3. Elliptic Curve Cryptography (ECC)

One of the popular Asymmetric key cryptography type is ECC .It is based on elliptic curve (EC) over finite fields, Neal Koblitz from (University of Washington) and Victor Miller from (IBM) in 1985 proposed the ECC algorithms [2]. An elliptic curve is represented as a loop of intersecting lines between the two axes. Multiplying a number by a point on the curve will produce other points on the curve, you have to know that even if the result and the original point are known but it is very hard to get the points [6].When comparing ECC to other public key cryptographic systems such as Rivest Shamir Adleman (RSA), we note that ECC has gained popularity in recent years due to its low overhead, low power and storage requirements, fast computations, and low bandwidth requirements [7].The popularity of Elliptic Curve Discrete Logarithm Problem (ECDLP) stems from the fact that it needs runtime that completely exponential, whereas the Integer-Factorization Problem (IFP) in other algorithms just requires part of the exponential runtime . Equation 3 show how to compute public key [8].

$$Pk = PV * G. \ldots\ldots\ldots\ldots (3)$$

Equation 3 is the principle of all elliptical curve cipher systems, in which both keys (PV, PK) are generated. Point multiplication or standard multiplication is the well-known name for this process which consumes most of the time taken by the whole system in the ECC algorithm, This means that even if we have the domain of an elliptical curve (which we will explain in detail later), the parameters, the generator (G) representing the generation points on the curve and the public key representing a point on the curve, it is still very difficult to determine the private key even if the value of public key is announced to all.

One of the most prominent features of the ECC encryption algorithm is that it maintains the same level of security with other algorithms, but with fewer keys. This explains the attraction towards its use, especially with large data [9] [8].

3.1 Arithmetic Background of Elliptic Curve

An elliptical curve can be represented by a cubic equation consisting of two variables with coefficients as shown in equation (4). The coefficients and parameters of an elliptic curve used for cryptography are limited to a finite Abelian group [10] [11]. A finite group is one that contains a limited numbers of items depending on the order of group (G). From a set of group G with the binary operation we can form the Abelian group $*: G \times G \rightarrow G$ .An elliptic curve equation for real number called Weierstrass equations [12] . As shown in figure 1:

$$y\text{^}2 = x\text{^}3 + ax + b \quad \ldots\ldots\ldots (4)$$

Equations of ECC achieve a condition:

$$4a^3 + 27b^2 \neq 0 \quad \ldots\ldots\ldots \quad (5)$$

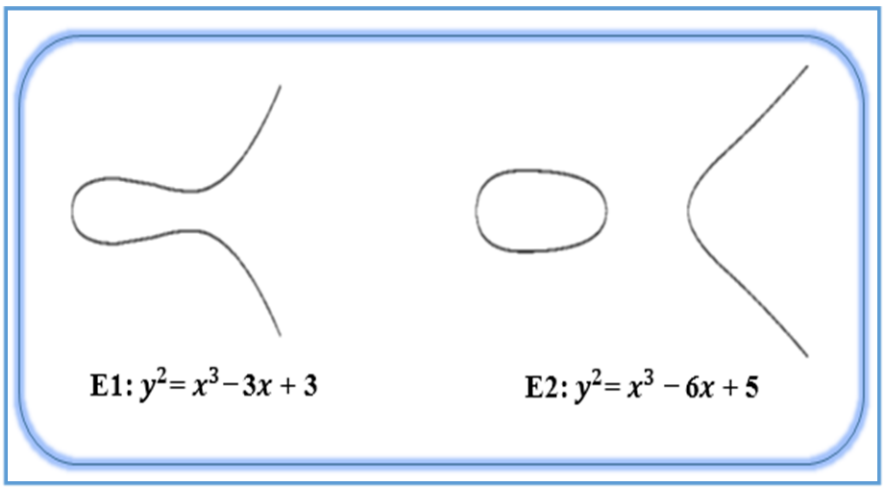

FIGURE 1: Elliptic Curves Examples

3.2 Elliptic Curves Operations:

3.2.1 Point Addition P + Q :

Suppose P, Q are points on EC, to obtain the point (R) on EC from these points, we must compute the point addition rule so: R (new point) = P + Q where P ≠ Q. In this example, a line will be drawn between the point (P) and the point (Q), point(R) is the mirrored point on the x-axis of the point obtained by intersecting the line with an elliptic curve. Figure (2) depicts an elliptic curve with an addition point [2], [13].

3.2.2 Point Doubling P+P:

To obtain the point R on EC we can compute new point(R) = point (P) + point (Q) since the criteria for this operation is that the points Q and P are equal (Q = P). So, We can say that R = (P) + (P) = 2P. In this case the tangent line will be drawn through P and get another point from the intersection between an elliptic curve and this line. Then mirror the resulting point of intersection on x-axis. This point results from mirroring the point R which results from the doubling. Figure (3) explains point doubling on an elliptic curve [2], [13]. .

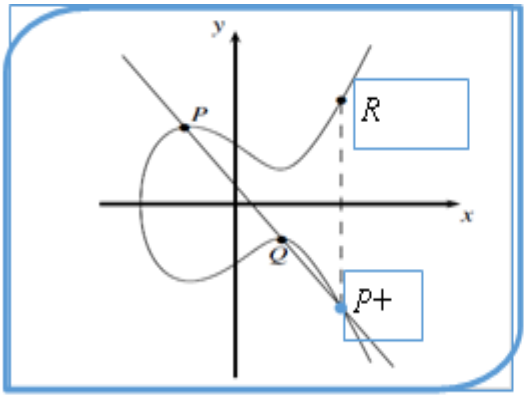

FIGURE 2: Point Doubling on ECC over $\mathbb{Z}$

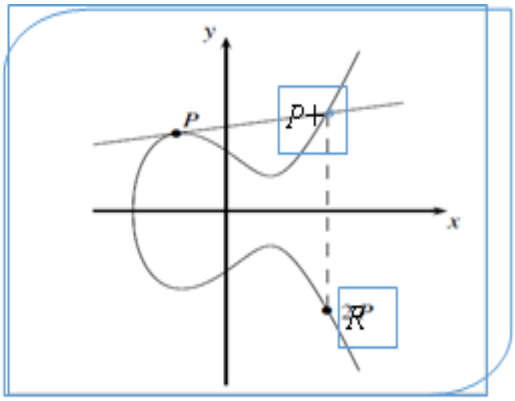

FIGURE 3: Point Doubling on an ECC over $\mathbb{Z}$

3.2.3 Point multiplication

The difficulty of addressing the elliptic curve discrete logarithm issue underpins the security of elliptic curve encryption. Point multiplication, also known as scalar multiplication, is the most common operation on the points of an elliptic curve. This entails adding P to itself Ks times for a given point P on the curve E and a specified scalar (Ks). This explains why ECDLP is complicated to fix. as indicated below[3], [13]:

QK =Ks * P= P+P+P+P+P+P+P

ks times.

3.3 Elliptic Curve Key Generation

Assume that E is an elliptic curve with a finite field Fp. Assume that P is a point in E(Fp), and that P has prime order n. The cyclic subgroup of E(Fp) generated by P is then:

$$\langle P\rangle = \{\infty, P, 2P, 3P \ldots (n-1)P\}$$

The public domain parameters are the equation of an elliptic curve E, prime p, and the point P and its rank n. A private key is an integer d that is selected randomly through the interval [1,n–1], and the public key that corresponds to d is Q = dP. The problem of determining d when giving Q and the domain parameters is an elliptic curve discrete logarithm problem (ECDLP) [9], [14].

3.4 Representing Plaintext

A way to translate a message into a point on an elliptic curve is necessary in order to employ elliptic curves. Following that, elliptic curve cryptosystems will be using elliptic curve methods to these points in order to generate new points that will serve as the ciphertext. To write points on an elliptic curve E, there is no known t polynomial time (mod p). There are, however, quick probability methods for finding spots that can be used to encrypt data. These approaches have the attribute of failing to create a point with a little probability. This chance may be made arbitrarily tiny, say on the order of 1/230, by correctly picking parameters. One encoding method, known as the Koblitz method, is as follows [15]:

- Let $E: y^2 = x^3 + ax + b \ (mod\ p)$ be an elliptic curve.
- M is a message that is mapped as a number, and J is a large integer where a failure rate of $1/2^J$ is acceptable when attempting to represent a message as a point. Suppose that M satisfies $(M + 1)\,J < p$. The message M will be represented by a number $x = M\,J+i$, where $0 < i < J$. For $i = 0, 1, \ldots, J\text{-}1$, compute $x^3 + ax + b$ and try to calculate the square root of $x^3 + ax + b \ (mod\ p)$.

If y has a square root, then Pm=(x,y) is calculated; otherwise, I is incremented by one and the process is repeated with the new value of x. This is performed until a square root is found or i= J. A message cannot be represented as a point if I ever equals J. To recover the message from the point $P_m=(x,y)$, it is simple to compute M as $M = \lfloor x/J \rfloor$, where x/J denotes to the largest integer less than or equal to x/J [15].

3.5 Elliptic Curve Encryption/Decryption

The encryption/decryption process in ECC only works on points, therefore the whole first stage (called Encoding) is to turn a normal text message m into such a point P(xy) on the curve to generate Pm, and then apply the encryption procedure to obtain Cm. The cypher point Cm is decrypted by first obtaining the plain point Pm, then decoding the point Pm to obtain the plaintext message m. The following describes the encryption/decryption process between two parties (Alice/Bob) using the ECC algorithm [8], [14]:

- Alice and Bob concur on the domain parameters (p, a, b, and a base point (G)) for constructing an E over a finite field GFp.
- Alice and Bob choose their respective private keys (da and db). The value of the private key must fall below |G| (the number of points generated from the base point) and within the range [1 - |G|].
- Find Alice and Bob's public keys (Qa and Qb) by multiplying their private keys with the base point as shown below:

$$Q_a = d_a \times G \mod p \quad (19)$$

$$Q_b = d_b \times G \mod p \quad (20)$$

- Alice first encrypts the message m into the point P_m, then chooses a random positive number in the range [1 - |G|] to use as a mask for multiplying with G and Q_b, and finally encrypts Pm with Bob's public key.

$$C_m = \{dG\ ,\ P_m + dQ_b\} \quad (21)$$

- To decrypt the received encrypted pair points Cm by Bob, he multiplies the first point ($\boldsymbol{dG}$) from the pair of Cm with his private key db and subtracted from the second point in the pair of Cm ($P_m + dP_b$).

$$P_m = P_m + k \times Q_b - d_b \times k \times G \quad (22)$$

- Finally, decoding Pm to obtain the massage [9], [16].

3.6 Various ECC Implementation and applications

In today's digital environment, little gadgets are extremely important. However, those devices have limited memory, and they also necessitate security, it presents a challenge because security demands precise adherence to specifications. ECC is considered the most appropriate cryptography for limited memory devices such as palmtops, smartcards, Smartphones, and other devices that use scalar multiplication, point addition, and point doubling [14] due to its small key size, limited operations, and small encryption and decryption parameters. For example, ECC was implemented in Radio Frequency Identification (RFID) and demonstrated to provide actual security for communication and data accessing marked memory. Furthermore, it reduces the amount of storage necessary for the key and the backend system by simply keeping the private key. As a result, the tag's commutation is reduced [14]. Additionally. ECC is popular public-key cryptography that may be used in mobile or wireless settings [17].

ECC is used in a variety of fields and systems in the real world. Bitcoin needs payment encryption to be sent straight from one peer to another without going via a financial institution. The public blockchain in Bitcoin is a collection of everyday Bitcoin transactions. Every block in this group carries an SHA-256 hash of the previous block, therefore the chaining of blocks begins with the origin block [18]. Secure Shell (SSH) employs ECC for server/client self-authentication by signing a replica of the exchange key, and ECDSA can be the key; clients can then use ECDSA as public keys for client authentication[18]. Austrian e-ID is a way of granting access to users through the use of physical smart cards. Cryptographic hardware modules are included in the smart cards, which carry a private key for encryption and signing. ECC has a smaller key size and lowers computational complexity [18]. The certificates of Transport Layer Security (TLS) consists of a kind of a public key in a way that the server uses to authenticate itself, and ECDSA can be that public key. TLS included ECC in the client/server greeting messages as well as a new set of cypher suites [12], [18].

4. Review with Discussion

Nine published papers and works for recent four years are reviewed, they are studied regarding some important categories: encrypted data type that applied on, protocols and algorithms that used in presented generators, then the efficiency measurements for testing the systems.

Furthermore, the results of each protocol are discussed separately according to security, consuming time, robustness against known attack types. Table 1,2,3,4 lists the main and most recent research progress of ECC protocols developed in the literature for solving data security and confidentiality problems.

Table 1 Elliptic curve works with audio

Author	Year	Data Type	Protocol	Measurement	Result
[19]	2019	Audio	Encrypt audio algorithm combining 1) chaotic system 2) DNA coding to confuse and diffuse the audio data	1)key sensitivity analysis 2) key-space analysis 3) spectrogram analysis 4) correlation analysis 5) PSNR test 6) simulation tools result 7)Running time and speed test 8) Histogram analysis 9) differential attack analysis	These algorithms were utilized for single and 2 different audio encryption and were found to have a wide key space, high key sensitivity, and resistance to different assaults through simulation tests and security research. As a result, the algorithm implementation may be applied to speech encryption.
[20]	2020	Audio	Encryption method using improved ElGamal Public Key.	1)Execution Speed 2)Key Space 3)Correlation coefcient for plain and cipher audio 4) Key Sensitivity 5) Spectrogram Analysis 6) Histogram Analysis 7) Diferential Attacks 8) Performance Analysis	For audio encryption, suggested an efficient public-key encryption strategy based on ECC and obtained an excellent execution speed for a public key encryption framework. The suggested approach is a robust, dependable public key audio encryption strategy owing to the analysis results, ECDLP strength, and ElGamal PKE enhancement.

Table 2 Elliptic curve works with image

Author	Year	Data Type	Protocol	Measurement	Result
[21]	2018	Image	1) ECC and chaotic system based asymmetric picture encryption method	1)key space 2)histogram 3)correlation 4)differential attack 5)Entropy	The suggested technique made key management and transmission reasonably easy and safe. The suggested method was shown to be safe enough to withstand brute force, differentiated attack, chosen

Author	Year	Data Type	Protocol	Measurement	Result
				6)encryption speed 7) Known plaintext attack.	plaintext assault, and statistics attack, according to experimental results and algorithm analysis.
[22]	2021	Image	Hybrid between Image encryption techniques using ECC with Hilbert matrix.	1) PSNR 2)UACI	ECC provides equal security with such a smaller key size and excellent PSNR and UACI results, making it difficult for an attacker to retrieve plain image.

Table 3 Elliptic curve works with some electronic media

Author	Year	Data Type	Protocol	Measurement	Result
[23]	2020	E-Payment	1)Encryption mobile payment using ECC with binary field for getting higher security 2) Text payment gatewa had been registration an mapped to elliptic curve points using ASCII values to be encrypted. 3) The gateway stores payment information, and can only be decodec using the decryption key provided by the merchant.	1)Key size 2)Computational power 3)Memory capacity 4)Encryption and decryption time 5)mobile battery	The suggested approach was found to ensure integrity, confidentiality, and privacy. The results further reveal that the suggested approach was time-efficient and computationally cheap in resource-constrained environments such as mobile payment systems.
[24]	2022	Electronic documentation	1)1st digital Signature generation algorithm based on elliptic curves 2)1st digital Signature verification algorithm 3)2nd Algorithm for generating signatures based on elliptic curves 4) 2st digital Signature verification algorithm		The article proposed and proves the correctness of new two stage digital signature algorithms with their verification based on the complexity of the discrete logarithm on elliptic curves.

Table 4 Elliptic curve works with video

Author	Year	Data Type	Protocol	Measurement	Result
[25]	2021	Video Conference	1) Using the ECIES encryption method to create secure video conferencing	1) Hash function 2) MAC function	A software program has been created that enable people to create secured virtual meetings using the ECIES encryption method on elliptic curves, enabling them to have meetings

Author	Year	Data Type	Protocol	Measurement	Result
			2) The Diffie–Hellman algorithm is used to transmit secret keys.		without worry of being hacked. As a result, the suggested application will considerably increase security services, personal data protection, and secret talks security. The program product developed may be used to perform secure video conferences.

ACKNOWLEDGEMENT

None

FUNDING

No funding received for this work.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] I. A. Taqi and S. M. Hameed, “A new Color image encryption based on multi chaotic maps,” *Iraqi J. Sci.*, vol. 59, no. 4, pp. 2117–2127, 2018, doi: 10.24996/IJS.2018.59.4B.17.

[2] K. E. Abdullah and N. H. M. Ali, “A secure enhancement for encoding/ decoding data using Elliptic Curve Cryptography,” *Iraqi J. Sci.*, vol. 59, no. 1 A, pp. 189–198, 2018, doi: 10.24996/IJS.2018.59.1A.20.

[3] M. Moshinsky, “Advances in Elliptic Curve Cryptography”, vol. 13, no. 1. 1959.

[4] R. Ariana, *済無No Title No Title No Title*. 2016.

[5] H. Cohen, “Handbook of Elliptic and Hyperelliptic Curve Cryptography - Google Books,” *Taylor & Francis Group*, 2005.

[6] C. Rebeiro, “Architecture Explorations for Elliptic Curve Cryptography on Fpgas Master of Science Thesis Certificate Acknowledgements,” no. February, 2009.

[7] B. Rashidi, “A Survey on Hardware Implementations of Elliptic Curve Cryptosystems,” no. December, pp. 1–61, 2017.

[8] K. Gupta, S. Silakari, R. Gupta, and S. A. Khan, “An ethical way for image encryption using ECC,” *2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009*, pp. 342–345, 2009, doi: 10.1109/CICSYN.2009.33.

[9] A. M. Sagheer, “Elliptic curves cryptographic techniques,” *6th Int. Conf. Signal Process. Commun. Syst. ICSPCS 2012 - Proc.*, no. December 2012, 2012, doi: 10.1109/ICSPCS.2012.6507952.

[10] W. Stallings, *C Ryptography and*. 2017.

[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. 2004. doi: 10.1007/b97644.

[12] N. T. Hussein and A. H. Kashmar, “An Improvement of ECDSA Weak Randomness in Blockchain,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 928, no. 3, 2020, doi: 10.1088/1757-899X/928/3/032022.

[13] A. M. Abdul-Hadi, Y. abdul-sahib Saif-aldeen, and F. G. Tawfeeq, “Performance Evaluation of Scalar Multiplication in Elliptic Curve Cryptography Implementation using Different Multipliers Over Binary Field GF (2233),” *J. Eng.*, vol. 26, no. 9, pp. 45–64, 2020, doi: 10.31026/j.eng.2020.09.04.

[14] D. Mahto and D. Kumar Yadav, “Performance Analysis of RSA and Elliptic Curve Cryptography,” *Int. J. Netw. Secur.*, vol. 20, no. 4, pp. 625–635, 2018, doi: 10.6633/IJNS.201807.

[15] Wade Trappe and L. C. Washington, “I n t r o d u c t i o n to C r y p t o g r a p h y w ith Coding Theory”.

[16] K. E. Abdullah and N. H. M. Ali, “Security improvement in elliptic curve cryptography,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 5, pp. 122–131, 2018, doi: 10.14569/IJACSA.2018.090516.

[17] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, “Elliptic curve cryptography in practice,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8437, pp. 157–175, 2014, doi: 10.1007/978-3-662-45472-5_11.

[18] M. Dubal and A. Deshmukh, “Achieving Authentication and Integrity using Elliptic Curve Cryptography Architecture,” *Int. J. Comput. Appl.*, vol. 69, no. 24, pp. 11–15, 2013, doi: 10.5120/12118-8141.

[19] X. Wang and Y. Su, “An Audio Encryption Algorithm Based on DNA Coding and Chaotic System,” *IEEE Access*, vol. 8, pp. 9260–9270, 2020, doi: 10.1109/ACCESS.2019.2963329.

[20] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. Al-Din Abed, and A. T. Hammid, “Implementation of El-Gamal algorithm for speech signals encryption and decryption,” *Procedia Comput. Sci.*, vol. 167, no. Iccids 2019, pp. 1028–1037, 2020, doi: 10.1016/j.procs.2020.03.402.

[21] X. Zhang and X. Wang, “Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem,” *IEEE Access*, vol. 6, pp. 70025–70034, 2018, doi: 10.1109/ACCESS.2018.2879844.

[22] Z. K. Obaidand and N. F. H. Al Saffar, “Image encryption based on elliptic curve cryptosystem,” *Int. J. Electr. Comput. Eng.*, vol. 11, no. 2, pp. 1293–1302, 2021, doi: 10.11591/ijece.v11i2.pp1293-1302.

[23] O. R. Vincent, T. M. Okediran, A. A. Abayomi-Alli, and O. J. Adeniran, “An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security,” *SN Comput. Sci.*, vol. 1, no. 2, pp. 1–12, 2020, doi: 10.1007/s42979-020-00122-1.

[24] M. Aripov and D. Kuryazov, “New Algorithms for Electronic Digital Elliptic Curves,” *Appl. Math. Inf. Sci.*, vol. 16, no. 1, pp. 121–125, 2022, doi: 10.18576/amis/160112.

[25] O. Safaryan *et al.*, “Video Conference Software Inplementation Based on Data Encryption Using Elliptic Curves,” *J. Phys. Conf. Ser.*, vol. 2131, no. 3, pp. 0–8, 2021, doi: 10.1088/1742-6596/2131/3/032112.