# Security Measures for Ensuring Confidentiality of Information Using Encryption by Elliptic Curve with Precomputation

Fatimah Dawoud Mousay
*Department of Mathematics*
The Libyan Academy
Benghazi, Libya
Alhotifatima@gmail.com

Souad I. Mugassabi
*Department of Mathematics*
*University of Benghazi*
Benghazi, Libya
Souad.Mugassabi@uob.edu.ly

Asma Ail Budalal
*Department Of Communication Technology*
*College Of Electrical And Electronic Engineering Technology Benghazi, Libya*
asma.budalal@.ceet.edu.ly

2023 IEEE 11th International Conference on Systems and Control (ICSC) | 979-8-3503-0488-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSC58660.2023.10449816

***Abstract*— Ensuring data confidentiality is crucial for all institutions. Providing a secure and fast system is needed to enhance confidentiality. Information security measures should also be identified and implemented to ensure the confidentiality of information security IS data. In this regard, whether the information is confidential during all stages of information capture, processing, storage, and transmission in IS is questionable, and challenging will face enhanced confidentiality. Many techniques have been proposed to protect data confidentiality. One of the best ways to protect data confidentiality is encryption. It is among the most powerful cryptography techniques elliptic curve cryptography (ECC) is available. Elliptic curve cryptography (ECC) is actively researched, and performance for EC-El Gamal is effective and uncomplicated. Public-key cryptography uses the ECC encryption system for asymmetric key encryption. Two parties can communicate simply by generating a public and private key securely. A more secure way to store and retrieve database information that is both convenient and efficient has been created. In this study, some constraints have been executed, preventing any unauthorized system from knowing the usual items used in encryption. Significantly, it will increase the security of information between two parts of communication if we keep some constraints unannounced in public; that is a certain way to save information from any attacks in advance.**

**Keywords— Information security, Confidentiality of IS, Elliptic curve cryptography ($ECC$). Elliptic curve over Finite field $E(F_p)$. Elliptic curve discrete logarithm problem ($ECDLP$). Number of points on elliptic curve ($N$).**

## I. INTRODUCTION

Advancements in information and communication technology (ICT) have led to the development of a versatile means of communication. In the field of information security, one of the crucial objectives is to protect privacy and proprietary information by strengthening confidentiality. In the context of information security, the confidentiality of information depends on implementing effective security measures and the proper configuration of settings. These measures are necessary to protect information throughout various stages, such as storage, processing, capturing, and transmission. Unauthorized disclosure of sensitive data and information can occur if confidentiality is breached. Confidentiality aims to prevent both deliberate and unintentional unauthorized access or observation of the contents of information [1-3]. A breach of confidentiality can happen when data or information is revealed, accessed, observed, monitored, acquired, or copied without authorization. There are various methods through which confidentiality can be compromised, including phishing attacks, identity theft, malicious attacks (such as computer viruses, Trojans, and worms), leaks of confidential information by insiders, security misconfigurations, weak authentication and access controls, SQL injections, cross-site scripting, and XPath injections.

There are several ways that sensitive information can leak, including malicious activities, technical methods, and non-technical methods. The loss of confidentiality is never easy to deal with and difficult to detect or track as information or data can be viewed/read or copied without leaving any trackback or footprint to track upon. Researchers are seeking solutions to the problem of a breach of confidentiality during information states. [3,4]. Some methods and strategies that have been applied in addressing confidentiality breaches such as cryptographic techniques, usually encryption [5].

## II. RELATED WORK

Numerous studies have addressed the issue of confidentiality in information systems (IS) and proposed various solutions. These studies emphasize the increasing importance of information encryption at the physical layer [6,7]. Encryption can be achieved through either asymmetric encryption or symmetric encryption [9,10].

Asymmetric encryption, also known as public cryptography, involves using different keys (a public key and a private key

979-8-3503-2521-10/23/$31.00 © 2023 IEEE



Authorized licensed use limited to: Trial User - Tec Monterrey (formerly ITESM). Downloaded on May 28,2025 at 14:21:41 UTC from IEEE Xplore. Restrictions apply.

pair) for encrypting plaintext and decrypting ciphertext. Commonly used asymmetric algorithms include the RSA (Rivest, Shamir, Adleman) algorithm, the and Elliptic Curve Cryptography (ECC).

On the other hand, symmetric encryption, also known as secret encryption/cryptography, uses the same key for both encrypting plaintext and decrypting ciphertext. Examples of symmetric encryption algorithms are 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard) [9,10].

According to [11], the use of precise elliptic curve cryptography (PECC) is based on algebraic elliptic curves in finite fields. The authors emphasize that PECC allows for secure data exchange through the use of reliable data consolidation methods that rely entirely on techniques for concealing rewritable data. Additionally, their research indicates that this approach surpasses data mining when it comes to implementing robust privacy measures without compromising data quality. Various performance metrics, such as average approximation error, computational cost, anonymizing time, and data loss, were thoroughly examined. The experimental results indicate that the proposed approach is both practical and applicable in real-world scenarios [11].

## III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography has a significant impact on secure information for its advantage depending on the struggle of solving discrete logarithm problems rather than RSA which depends on factorization problem, consequently, ECC has higher strength-per-bit. Due to the advantages of compactness and efficiency, it has emerged as the preferred cryptography for mobile computing and communications devices. However, there are several methods that attack the ECC and work for a general finite group such as Baby-step, Giant-step, Pohlig-hellman, Pollards $\rho, \gamma$ and Mov attack. The most important is Baby-step, Giant-step due to its effectiveness which can be proven mathematically. In [12, 13] chose a very small number $p$ to explain how to hide data within an image and image encryption respectively. During [14] choosing $N$ and $k$ to be very large numbers nevertheless a large key space is only a necessary but not a sufficient condition for a secure system cipher. The cipher must also be strong against analytical attacks [15]. In [16] proposed steps to decrease attacks, the authors refer to combination of the Pohlig-Hellman and Pollards $\rho$,as the best general known attack on ECC is choosing $N$ to be ca composite of large prime numbers has divisor $\geq 2^{160}$ to prevent Chinese Remainder Theorem to be applied leads to Pohlig-Hellman to be unsuccessful. However, solving congruence equations by Chinese Remainder Theorem requires many conditions and the possibility of the Pollards $\rho$ method makes Baby-step giant-step the most important method. Anomalous curve is elliptic curve E($F_p$) with $N = p$. It is easy to solve DLP through it for more information see [17].

### A. Group And Field

A collection of points with one operation that has special properties such closure, associativity, and existence of identity element and an inverse of each element is called a group, when the previous properties hold with commutativity property under two operations is called a field.

### B. Finite Field

A finite field with a characteristic and number of elements equal $p$ defined as

$$F_P = \{a \ mod \ p : a = 0,1,2 \ldots, p-1\}.$$

For any integer number $b$ where $0 < b < p-1$, we have $b = a + kp$ for some integer $k$, which means $b \equiv a \ mod \ p$.

For example

$F_5 = \{0,1,2,3,4\}$ , $9 = 5 \times 1 + 4$ so $9 \equiv 4 \ mod$ and $-3 = 2 + 5 \times (-1)$ hence $9 \equiv 4 \ mod \ 5$ and $-3 \equiv 2 \ mod \ 5$.

Theorem (1)

The system of linear congruent equation of the form

$$ax + by = e \ mod \ m$$

$$cx + dy = f \ mod \ m$$

Has an only one solution if the greatest common divisor between $m, ad - bc$ is 1. See [18].

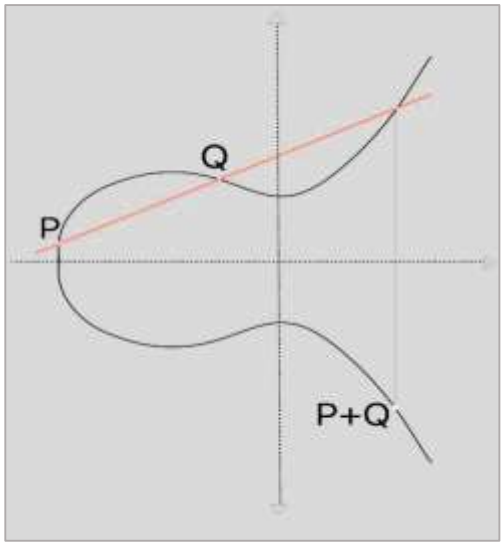
### C. Elliptic Curve

The elliptic curve is a nonsingular smooth projective curve over a field defined as

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

where $4a^3 + 27b^2 \neq 0$.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are pointes in elliptic curve (1). The addition operation define as $P + Q = (x_3, y_3)$ (See Figure 1)






Authorized licensed use limited to: Trial User - Tec Monterrey (formerly ITESM). Downloaded on May 28,2025 at 14:21:41 UTC from IEEE Xplore. Restrictions apply.

Figure 1: The geometric meaning of adding two points ($P$ and $Q$) in the elliptic curve.

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$$

where

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = -[m^2(x_3 - x_1) + y_1]$$

If $P \neq Q$ then

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \quad (2)$$

and if $P = Q$ we have

$$m = \frac{3x^2 + a}{2y}. \quad (3)$$

and $-P = -(x_1, y_1) = (x_1, -y_1)$

The points satisfy equation (1) are called points on elliptic curve with a point at infinity $O$ collect a group with previous operation.

The elliptic curve over finite filed $F_p$ is $E(F_p): y^2 \equiv x^3 + ax + b \bmod p$.

Example (1)

The points on $y^2 = x^3 + x - 1 \bmod 3$ are

| $x$ | $y$ | $P$ |
|---|---|---|
| 0 | $-$ | $-$ |
| 1 | 1 | (1,1) |
| | $-1$ | $(1,-1) = (1,2)$ |
| 2 | 3 | $(2,3) = (2,0)$ |
| | $-3$ | $(2,-3) = (2,0)$ |

$E(F_3) = \{O, (1,1), (1,2), (2,0)\}$. See [19]

In figure 2 we can see that $(1,1)$ is the generator of $E(F_3)$

```
18) gp > H=ellgenerators(E1)
 [[1, 1]]
18) gp > oH=ellorder(E1,[Mod(1,3),Mod(1,3)])
 4
```

Figure 2: Using PARI/GP to find the generator (1,1).

Note that: There are $N + 1 - t$ points on $E(F_p)$ where $t \leq 2\sqrt{p}$ according to Hasse's theorem.

*D. Supersingular Elliptic Curve*

The elliptic curve over the finite field is called supersingular if $N = p$ otherwise is called ordinary. DLP over supersingular $E(F_p)$ readily resolved by the MOV attack which depends on pairing.

*E. Discreet Logarithm Problem On Elliptic Curve*

The ability to solve DLP using a variety of methods is the main problem of being encryption by elliptic curve on attack i.e., finding integer $k$ from $Q = kP$.

Note that: $kP$ refers to repeating addition of $k$-times

*F. Baby- Step, Giant -Step*

Baby-step giant-step is a certain method to solve any ECCDL so it represented to be very strong attack because there is always a match between points which we have to store and the actual value of $kP$ In many cases, it is an effective and fast method to solve any ECCDL over $F_p$ when $p$ is a small prime number. Although it requires plenty of storage until we get a match that make it an unfavorable method when $p$ is extremely large. Steps follow as

1) Suppose $Q = kP$ where $k$ is integer and $P, Q$ points on $E(F_p)$.

2) Choose $n \geq \sqrt{N}$ then compute and store $iP$ where $0 \leq i < n$ then calculate $Q - jnP$ with $0 \leq j \leq n - 1$ so we continually get a point such that $iP = Q - jnP$.

*G. El Gamal Public Key Encryption*

The protocol proposed by Taher El Gamal depends on EC Difffie-Hellman key agreement protocol being one of these public-key-encryption is widely used for asymmetric cryptosystem. Steps listed as:

Suppose that Alice went to send a message to Bob.

1) *Generation*

Bob chooses equation $E(a, b)$, large prime number $p$, generator point $P(x, y)$ in $E(a, b)$, integer $k$ and he calculates $Q = kP$ then announces all except $k$ (private key).

2) *Encryption*

Alice chooses a private key $r$ ($r$ is integer) and calculates her public key $rP$ and constructs the ciphertext $C$ where $C = M + rQ$ ($M$ is plaintext in $E(a, b)$) then sends to Bob.

3) *Decryption*

Bob can derive to the plaintext by $M = C - rQ$ where $rQ = rkP = krP$.

## IV. PRECOMBUTATION

Choosing the ordinary elliptic curve $E(F_p)$ where $p$, $N$ is a large prime, large composite number respectively in order to decreases the impact of Pohling-Hellman, also the attacks from Pollards $\rho$ and $\lambda$ methods require $N$ to be prime best. Thus Baby-step giant-step unaffective due to a large number



Authorized licensed use limited to: Trial User - Tec Monterrey (formerly ITESM). Downloaded on May 28,2025 at 14:21:41 UTC from IEEE Xplore. Restrictions apply.

of storages needed. Second, according to the uniqueness of least common multiple ( $lcm$ ) and some mathematical approaches enable us to achieve this method.

Suppose

$$E: Y^2 = X^3 + \frac{a}{n}X + \frac{b}{m} \ mod\ p$$

where $p$ is a large prime number.

Let $l = \acute{n}lcm(n, m)$ where $\acute{n}$ is integer $X = \frac{x}{l^2}$ and $Y = \frac{y}{l^3}$.

Hence

$$y^2 = x^3 + Ax + B \ \ mod\ p. \qquad (4)$$

Where $A = \frac{a}{n}l^4$ and $B = \frac{b}{m}l^6$ are integers, (4) the actual equation

Note that: the usual procedure when we have fractional coefficients is to find the multiplicative inverse in $mod\ p$ of the denominator $n$ and $m$ then multiply by $a$ and $b$ respectively that results in an unused equation.

Before transmission, (as shown briefly in Figure (3) convert all points to fractional form, else would become this method on attack of knowing the actual equation by using any two points to solve two congruence equation. Since $p$ is prime number and according to theorem (1) the equation has a unique solution.

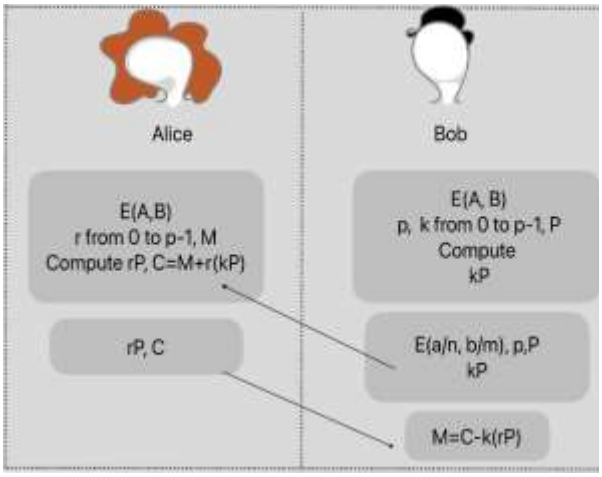



Figure 3

Example (2)

Use the Pari/GP calculator version 2.16.0.

Suppose Alice wants to send $M$ to Bob.

Contracted $\acute{n}$ to be 1 before communication.

Bob set

$E\left(\frac{7}{3}, \frac{2}{5}\right), p = 178987, P = (116485,32401), kP = (77925,61127)$

Bob announced

$$E\left(\frac{7}{3}, \frac{2}{5}\right), 178987, \left(\frac{116485}{\acute{n}15^2}, \frac{32401}{\acute{n}15^3}\right), \left(\frac{77925}{\acute{n}15^2}, \frac{61127}{\acute{n}15^3}\right)$$

and

$$E: y^2 = x^3 + \frac{7}{3}x + \frac{2}{5} \ \ mod\ 178987$$

So

$k = 229$ and $N = 178422 \neq p$, $lcm(3,5) = 15$.

Alice downloads what Bob has announced and prepares some precomputation by previous method as well as Bob did.

Let $x = \frac{X}{15^2}, \ \ y = \frac{Y}{15^3}$

From equation $E$

$$\left(\frac{Y}{15^3}\right)^2 = \left(\frac{X}{15^2}\right)^3 + \left(\frac{X}{15^2}\right)\frac{7}{3} + \frac{2}{5}$$

$Y^2 = X^3 + 118125X + 81575 \ \ mod\ 178987.$

Then she chooses her private key $r = 3621$ and the point $M = (47542,46746)$ then she calculates

$rP = (33611,25834)$

$M + \acute{n}\, rkP = (55478,6488).$

Bob can easily deduce $M$ after sending Alic to $rP, C$ in fractional form

$$(55478,6488) - \acute{n}\ krP$$
$$= (55478,6488) + (162048, -115035)$$
$$= (47542,46746)$$

where $(-115035)\ mod\ 178789 = 63952$.

If they transmit more than one point in integer formula then any unauthorized access can calculate the coefficients of the elliptic curve equation which is used both in encryption and decryption.

Suppose these points

$$(116485,32401) \text{ and } (47542,46746)$$

By substituting in equation (4)

$$85149 = 116485A + B \ mod\ 178987$$

$$69422 = 47542A + B \ mod\ 178987$$

It is fairly easy to identify the system's unique solution; however, converting the points formula is essential for this method to succeed.

## V. CONCLUSION

This method provides an unconventional way to strengthen the confidentiality of information using ECC and


Authorized licensed use limited to: Trial User - Tec Monterrey (formerly ITESM). Downloaded on May 28,2025 at 14:21:41 UTC from IEEE Xplore. Restrictions apply.

performs for symmetric and asymmetric algorithms. Attacks require the elliptic curve equation to be operated; therefore, using ECC will incredibly increase information security between two parts of communication. keeping some constraints unannounced in public, which can be considered a reliable way to save information from any attacks in advance. Hence, not announcing the actual elliptic curve equation (which needs precomputation and secret key $\acute{n}$ ) would enhance information security. In future work, speeding up extracting the point on an elliptic curve over the Galois field which will help communication parts speed up the authentication processes. Additionally, as mentioned in the previous analysis, the ECC is a good option among various cryptography over the Galois field as recommended in [20-21]. Thus, our future work will utilize the proposed mathematical approach in the teleoperated robotic system.

## ACKNOWLEDGMENT

The authors are grateful to Department of Mathematics in Libyan Academy, Department of Mathematics in University of Benghazi and the College of Electrical & Electronics Technology of Benghazi, Libya, and for supporting this research.

## REFERENCES

[1] Forbacha, Suh Charles, and Mbuya Josiah Anyam Agwu. (2023) "Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet)." American Journal of Technology 2, no. 1: 1-36.

[2] Yalew, Sileshi Demesie, Pedro Mendonca, Gerald Q. Maguire, Seif Haridi, and Miguel Correia. (2017) "TruApp: A TrustZone-based authenticity detection service for mobile apps." *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1-9.

[3] J Bosworth, Seymour, and Michel E. Kabay, eds. (2014) Computer security handbook. John Wiley & Sons.

[4] Syreyshchikova, Nelli V., Danil Yu Pimenov, Tadeusz Mikolajczyk, and Liviu Moldovan. (2019) "Information Safety Process Development According to ISO 27001 for an industrial enterprise." Procedia manufacturing 32: 278-285.

[5] Kessler, G. C. (2019). An Overview of Cryptography. Retrieved September 7, 2019,

[6] Nabeel, Mohamed. (2017) "The many faces of end-to-end encryption and their security analysis." *IEEE international conference on edge computing (EDGE)*, pp. 252-259. from https://www.garykessler.net/library/crypto.html#types R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[7] Sultan, Amber, Xuelin Yang, Syed B. Hussain, and Weisheng Hu. (2018) "Physical-layer data encryption using chaotic constellation rotation in OFDM-PON." In 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 446-448. IEEE.

[8] Varshney, G., Misra, M., & Atrey, P. (2018). A new secure authentication scheme for web login using BLE smart devices. In 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), 27-29 Oct. 2017, Xiamen, China (Vol. 2017-Octob, pp. 95–98).

[9] Lin, Han-Yu, and Yao-Min Hung. (2020)"An improved proxy Re-encryption scheme for IoT-based data outsourcing services in clouds." *Sensors* 21, no. 1: 67.

[10] Hussain, I., Negi, M. C., & Pandey, N. (2019). 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 29-31 August 2018, Noida, India, India. In 2018 7th

[11] Murugeshwari, B., D. Selvaraj, K. Sudharson, and S. Radhika. "Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography." Intelligent Automation & Soft Computing 35, no. 1 (2023).

[12] Mohanta, Hemanta Kumar. (2014) "Secure data hiding using elliptical curve cryptography and steganography." *International Journal of Computer Applications* 108, no. 3: 16-20.

[13] Obaid, Zahraa Kadhim, and Najlae Falah Hameed Al Saffar. (2021) "Image encryption based on elliptic curve cryptosystem." International Journal of Electrical and Computer Engineering 11, no. 2: 1293.IEEE..

[14] Rabah, Kefa. (2005) "Implementation of elliptic curve diffie-hellman and EC encryption schemes." *Information technology journal* 4, no. 2: 132-139.

[15] Christof, Paar. (2005) "Applied cryptography and data security." Ruhr-University Bochum/Germany.

[16] Sommerseth, Martin Lysoe, and Haakon Hoeiland. (2015) Pohlig-hellman applied in elliptic curve cryptography. Technical Report, University of California Santa Barbara. 2015. Available online: https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Sommerseth+ Hoeiland. pdf (accessed on 29 March 2020),

[17] Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. CRC press.

[18] Koshy, T. (2002). *Elementary number theory with applications*. Academic press.

[19] Lozano-Robledo, Á. (2011). *Elliptic curves, modular forms, and their L-functions* (Vol. 58). American Mathematical S

[20] López, Julio, and Ricardo Dahab. (1999)"Fast multiplication on elliptic curves over GF (2 m) without precomputation." In Cryptographic Hardware and Embedded Systems: First InternationalWorkshop, CHES'99 Worcester, MA, USA, August 12–13, 1999 Proceedings 1, pp. 316-327. Springer Berlin Heidelberg.

[21] Xiao, Yong, Weibin Lin, Yun Zhao, Chao Cui, and Ziwen Cai. (2021) "A high-speed elliptic curve cryptography processor for teleoperated systems security." Mathematical Problems in Engineering 2021: 1-8.



Authorized licensed use limited to: Trial User - Tec Monterrey (formerly ITESM). Downloaded on May 28,2025 at 14:21:41 UTC from IEEE Xplore. Restrictions apply.