

An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL

Josepha Menandas

Department of Networking and Communications
SRM Institute of Science and Technology Kattankulathur
India
jj0901@srmist.edu.in

Mary Subaja

Department of Networking and Communications
SRM Institute of Science and Technology Kattankulathur
India
marysubc@srmist.edu.in

Abstract: As the amount of data that is being generated and processed continues to grow in both volume and complexity, data security has become a critical problem. As cloud computing, Internet of Things (IoT) devices, and sophisticated cyber threats continue to grow in popularity, it is necessary to preserve data security through a multidimensional approach that can adapt to the ever-changing risks and technology. Prominent cryptographic algorithms primarily focus on ensuring confidentiality. To address additional parameters, it is necessary to explore algorithms such as signature algorithms for authentication and another algorithm for integrity. Here we introduce the novel approach of securely utilising the Transport Layer Security/Secure Socket Layer (TLS/SSL) protocol with a modified Elliptic Curve Cryptographic (ECC) algorithm which supports the security parameters of confidentiality, authentication and integrity. The main functionalities of establishing the secure connection after the Transmission Control Protocol (TCP) initiation, the handshake process, like cipher suite, authentication and generating a secret key for encryption use the novel modified ECC method with fewer steps when compared to existing TLS/SSL using Rivest Shamir Adleman algorithm (RSA) and other symmetric cryptographic algorithms. The performance is improved by leveraging the computational arithmetic over Elliptic Curve (EC) points for key generation with the Chinese Remainder Theorem (CRT) combined with double and add implementation and the effective hashing algorithm. Additionally, it offers enhanced resistance to Power Analysis Attacks (PAA) and Side Channel Attacks (SCA). Also, it has been demonstrated that the overall performance surpasses the current state of the art in existing solutions.

Keywords: Elliptic curve cryptography, transport layer security, confidentiality, authentication, integrity, chinese remainder theorem, hash algorithm, point arithmetic.

Received January 4, 2025; accepted June 23, 2025
<https://doi.org/10.34028/iajit/22/5/2>

1. Introduction

With speedier communication technologies, data security and privacy in transit are crucial concerns. Data confidentiality, computation and communication costs, and security concerns must all be taken into account [20]. Although there is a significant increase in data handling these days, secure data management is still a huge task. There are a lot of secure data handling solutions on the market today that don't fully adhere to security principles [11]. When compared to other public key methods such as Rivest Shamir Adleman algorithm (RSA), Diffie-Hellman, Digital Signature Algorithm (DSA), and others, Elliptic Curve Cryptography (ECC), which was developed by Miller [26] and Koblitz [18], offers the highest level of security. ECC uses a small length key although ECC offers robust security, its lack of authentication and integrity makes it unsuitable for real-time scenarios. ECC encryption is often performed on Elliptic Curve (EC) points, or text messages that have been converted into EC points. The cipher text is then created by simply adding the random variable that was created by the sender. It does not authenticate the sender

because the randomly generated value is used for encryption [30], it does not offer the message's integrity either. We created a revolutionary ECC-based encryption method that supports confidentiality, authentication, and integrity all at once because security parameters like these were lacking.

1.1. Elliptic Curve Overview

ECC is an asymmetric cryptographic algorithm that offers enhanced security even with smaller key sizes when compared to other algorithms [13]. The security level provided by a 160-bit key length in ECC is comparable to that of a 1028-bit key length in RSA [33]. The invention of Shor's algorithm for prime factorization has resulted in a reduction of security in RSA, highlighting potential threats. The symmetric key encryption algorithm, such as Advanced Encryption Standard (AES), provides high security; however, it suffers from performance issues when it comes to key exchange between the sender and receiver, and it is also vulnerable to Man In the Middle Attack (MIMA). Conversely, the application of ECC algorithms such as

ECC, Elliptic Curve Diffie Hellman algorithm (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA) effectively mitigates threats due to the complexities associated with Discrete Logarithmic Problems.

The Weierstrass Equation (1) for elliptic cubic curve [13, 19]

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

With $a_1, a_2, a_3, a_4, a_6 \in K$ and K is the point on EC field.

In general, the simplified ECC equation derived from Equation (1) is

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

And the singularity exists if and only if, $4a^3 + 27b^2 = 0$. Let $E_p(a, b)$ be the simple curve representation and $p \in \mathbb{Z} = \{0, 1, 2, \dots, p-1\}$. The point $P = (x_p, y_p)$ is the curve point proving the curve Equation (2). Form Equation (2), for $p > 3$, then

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

1.2. Properties of Cubic Curve Group

- Cycle property: an EC is said to be cycle if satisfies the finite group property like closure, associative, identity, inverse, and commutative.
- Galois field property: it is created by Galois [17], and is defined as the finite elements represented as $GF(P^n)$ where P^n be a prime or power of 2.
- Order property: number of points on curve (n) is called order property and it varied from

$$p + 1 - 2\sqrt{p} \text{ to } p + 1 + 2\sqrt{p} \quad (4)$$

- Discrete logarithm property: in RSA, modular multiplication corresponds to the addition operation in ECC, whereas modular exponentiation is analogous to multiple additions. It is essential to pinpoint a “hard problem” that parallels the task of factoring the product of two prime numbers or computing the discrete logarithm [17, 19] to develop a cryptographic system based on EC. From the EC points, Equation (5).

$$Q = kP \text{ where } Q, P \in E_p(a, b) \text{ and } k < P \quad (5)$$

Computing Q from k and P is relatively straightforward, whereas determining k from Q and P presents significant challenges. The problem at hand is the EC discrete logarithm problem. In RSA, modular multiplication corresponds to the addition operation in ECC, whereas modular exponentiation is analogous to multiple additions. It is essential to pinpoint a “hard problem” that parallels the task of factoring the product of two prime numbers or computing the discrete logarithm [17, 19] to develop a cryptographic system based on EC. From the EC points, the equation $Q=kP$ where $Q, P \in E_p(a, b)$ and k .

1.3. Galois Field of Cubic Curve

The $GF(P^n)$ is an exceptional representation of a finite

bounded grouping of elements. There are two methods of defining GF .

$$GF(P^n) = \begin{cases} GF(P) & \text{when } n = 1 \text{ and } P \text{ is prime} \\ GF(2^n) & \text{when } P = 2 \text{ or power of 2.} \end{cases} \quad (6)$$

In general, the polynomial of degree $n-1$ for GF is given as follows.

$$GF(P^n) = \bigcup_{n=1}^{n-1} \left\{ \int_{p=0}^{p-1} p \quad n \in \mathbb{Z}^+ \right. \quad (7)$$

The paper is organized as follows. Chapter 2 presents the foundational laws and the point arithmetic associated with ECC. Chapter 3 provides a comprehensive literature review along with an identification of the existing research gap. Chapter 4 provides an in-depth examination of the proposed algorithm, while chapter 5 presents the performance analysis, results of the proposed work, and an assessment of security against potential threats, concluding with a discussion on future work. Table 1 illustrates the expansion of various notations utilized in the paper.

Table 1. Notations and usages in the proposed work.

Symbol	Expansion
CRT	Chinese Remainder Theorem
CIA	Confidentiality, Integrity, Authentication
TLS	Transport Layer Security
FPGA	Field Programmable Gate Array
$E_p(a, b)$	Elliptic Curve
P_i	i^{th} point
P, Q, R	Points
(x_p, y_p)	Point representation on Elliptic Curve
$GF(P^n)$	Galois Field
G	Generator point
Δ	Slope (Calculate distance between points)
'O'	Point at infinity
XOR	Binary Operation
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
RSA	Rivest Shamir Adleman algorithm
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ASCII	American Standard Code for Information Interchange
$\cong$	Congruent
P_A, P_B or K_A, K_B	Public key
n_a, n_b	Private key
(C_1, C_2)	Cipher text pair
C_0, M_1, M_2	Parameters of Chinese Remainder Theorem

2. Elliptic Curves Point Arithmetic

The fundamental arithmetic operations of EC are point addition and Point Multiplication (PM). Addition is possible only if the points coordinates are different, and point doubling otherwise called PM is possible if point coordinates are same [18, 19, 26].

2.1. Primitive Law of Point Addition

The addition property defined as follows,

1. If $X_1=0$, then $X_1+X_2=X_2$, the same for $X_2=0$.
2. If $X_2=-X_1$, then $X_1+X_2=0$.
3. If $X_2=X_1$ then $X_1+X_2=X_3=(a_3, b_3)$ with $a_3=\Delta^2-2a_1$ and

$$b_3 = \Delta(a_1 - a_3) - b_1 \text{ for } \Delta = \frac{3a_1^2 + E \cdot b}{2b_1}.$$

4. If $X_2 \neq X_1$ then $X_1 + X_2 = X_3 = (a_3, b_3)$ with $a_3 = (\Delta^2 - a_1 - a_2)$ and $b_3 = \Delta(a_1 - a_3) - b_1$ for $\Delta = \frac{(b_1 - b_2)}{(a_1 - a_2)}$.

2.2. Primitive Law of Point Multiplication

PM also known as scalar multiplication, is represented by the Equation $X = kP$, which is the addition of point P

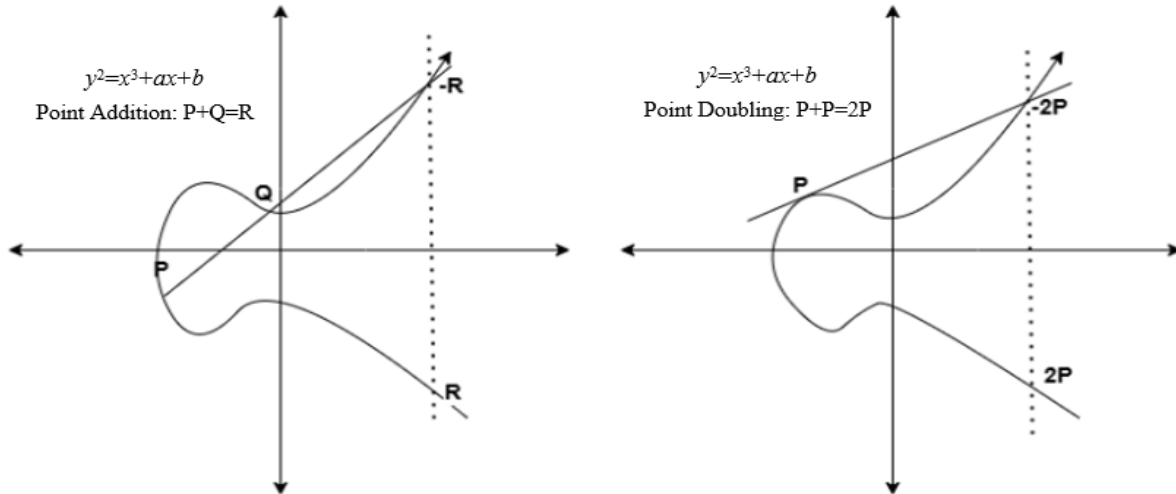


Figure 1. EC point arithmetic.

Hankerson *et al.* [13] employed a method called “double and add,” which uses the traditional way to calculate Equation (2). For a representation of m bits, the average of $(m/2)$ additions and (m) doublings is required. Multiplication can be calculated in a set amount of time using the montgomery ladder algorithm, which was first presented by Joye and Yen [15] and Ahmadi *et al.* [1]. This algorithm utilizes two registers, R0 and R1, based on the bit representation of k . When k_i is equal to 0, R1 is employed for point addition and R0 for point doubling. R0 and R1 are utilized interchangeably when k_i equals 1. A Non-Adjacent Form (NAF) representation utilizing direct doubling alongside a fixed-base comb technique was proposed by Tsaur and Chou [38]. In instances of multiple doubling, this facilitates efficient calculation of the table. An advanced approach employing a width- w NAF representation along with an alternative pre-computation table format was presented by Mohamed *et al.* [27]. Implementing an intelligent look-up table in conjunction with Mohamed *et al.*'s [27] method, Seo *et al.* [36] offer a strategy for efficient scalar multiplication. In order to compute scalar multiplication with less group addition operations, this structure generates successive zero-sequences more frequently. This characteristic is formed by analysing the w -NAF behaviour and evaluating secret scalars, k , which are provided by the blum-blum-shub random number generator. One method for quick scalar multiplication, proposed by Gallant *et al.* [10], makes use of the curve's endomorphism. To make calculating k_1 and k_2 easier, this feature incorporates the Standards for Efficient Cryptography Prime 256-bit curve Koblitz-1 (SECP256K1), which consists of λ and

by itself k times. For k times, $X = (P + P + P + \dots + P)$. The EC points arithmetic point addition and point doubling are graphically represented in Figure 1.

Various researches have been taken out in order to reduce the overall time complexity of EC algorithm. Normally EC time complexity depends only on the point arithmetic, especially for PM. There are various PM implementations in order to reduce the time complexity.

H. The average number of $m/2$ point doublings and $3m/8$ point additions needed for this strategy is 3. The average number of point-additions is reduced to $m/4$ when the Joint Sparse Form (JSF) [6] of k_1 and k_2 is followed. The Dynamic Binary Neural Network System (DBNS), or double-based number system, was proposed by Dimitrov and Cooklev [8]. There are no workable applications that result from the scalar multiplication representation. For integers between 40 and 50 bits, the approach works, but it takes exponentially long time. Similarly, this DBNS makes use of binary and ternary structures within a hierarchical tree-based implementation. In its expanded version, Directed Acyclic Graphs (DAGs) are used to implement DBNS. An improved DAG approach, called the L-T technique [6], has been used, leading to a considerable decrease in time complexity. Another technique that has been suggested using the Residue Number System (RNS) implementation is the tree-based L-T algorithm. We offer a new approach that combines the double-and-add method with the CRT.

2.3. Chinese Remainder Theorem (CRT)

By first reducing larger integers to smaller ones using divisors, the theorem can be applied to get the original number [9]. When divisors are coprime, this becomes feasible. It was finished in 1247 by Qin Jiushao after being described in 1236 by Sun Zi, a CRT. We can examine finite sequences of integers, characterize dedekind domains, and apply the CRT in cryptography methods. In other words, we can create a unique solution

to the system $x \pmod{pq}$ by combining two equations, and $x \pmod{q}$, where p and q are separate moduli. When handling big integers, the inverse approach is easy as pie. The inverse approach explains that, given a big $x \in \mathbb{Z}_{pq}$ we can simplify it by reducing it *modulo* p and $x \pmod{q}$, resulting in a pair of equations such as $x \pmod{p}$ and $x \pmod{q}$. Then, we can find the answer by solving for y as $aq_1 + bp_1 \pmod{pq}$, and y will fulfill the solution. Since a and b are relatively small in comparison to x , our suggested approach uses (a, b) instead of (x) to perform the necessary computations, and then returns the result in terms of (x) . This is done for $x \in \mathbb{Z}_{pq}$ which is used for scalar multiplication in text to point conversion. For many algorithms, including the EC method, this will significantly shorten the time it takes to do scalar multiplication.

3. Related Work

3.1. Literature Review

To lessen the load on LoRaWAN power supplies, Puckett *et al.* [29] presented cryptographic methods based on hardware. All three functions-encryption, decryption, and digital signature generation-are housed in the cryptographic coprocessor. Each node's total energy consumption is drastically cut because this configuration is hardcoded during production and cannot be changed. In order to decrease energy consumption, every node makes use of several cryptographic methods, such as AES, ECC, and Secure Hash Algorithm (SHA). Computing complexity increases due to differences in key setup for cryptographic approaches in implementations.

Oladipupo *et al.* [28] suggested a way to construct a Wireless Sensor Network (WSN) that does away with sensor clustering and instead makes use of multicore wireless sensor nodes. A variety of Elliptic Curve Cryptographic methods, such as ECC, ECDSA, Elliptic Curve Cryptography Diffie-Hellman (ECDH), etc., are employed to attain the safe communication. In order to strengthen security, Han *et al.* [12] introduced a new protocol for key agreement and multifactor authentication that makes use of symmetry key cryptographic algorithms that perform XOR operations. The Industrial Internet of Things (IIoT) security holes in the Rafique *et al.* [31] multi-factor authentication protocol are also made possible by this.

A novel protocol for authentication and key agreement was developed by Chen *et al.* [5]. This protocol makes use of the ECC method for encryption and decryption, which uses a hash function. The XOR operations on point arithmetic and the randomly generated numbers used to designate time to send and receive encrypted data help with all of this. The key regeneration, however, necessitates extensive implementation-level complexity. Li *et al.* [24] presented a biometric implemented authentication

technique that uses ECC in conjunction with fuzzy extractors and biometric hashing. They provided the proof that, the protocol has a very low likelihood of being attacked.

In order to circumvent the risks associated with WSN Wu *et al.* [41] suggested a novel approach to key generation for ECC algorithms based on the beta gamma function, [39] key generation becomes extremely laborious when dealing with extremely big numbers. Additionally, there is no determinism in ECC encryption using beta gamma key generation. An innovative approach to ECC was introduced by Dabholkar and Yow [7] for use with networked wireless sensor devices that have limited memory and power. This approach relies on a finite field curve, $f(2^n)$, and requires fewer processing resources suggested a method contains three-factor of authentication that generates keys. Additionally, the suggested technique encrypts data using AES, making safe key management challenging in WSNs. In order to increase the security of data transfer across an unprotected channel, Rafique *et al.* [31] suggested a certificateless protocol that uses symmetric key algorithm with XOR Boolean function and hashing to establish that the protocol is secure. Additionally, it has been demonstrated that, although it is quite safe for data transmission over an unsecured channel, password guessing attacks are possible due to the long key length and the difficulty of securely encrypting symmetric keys.

Shuai *et al.* [37] brought in an innovative secure authentication technique that eliminates the password recognition database by using Rabin cryptosystem integrating with forward anonymity for IIoT systems. The intensive evidence on a study indicates that it provides the required functional and security characteristics. With comparison to analogous stratagem, it attains an optimal security-efficiency balance that is perfect for practical applications. Zhang *et al.* [43] brought in a novel method that adds multifactor authentication with blockchain technology to improve the security robustness of multiparty interactions across devices across many domains. The various qualities are depicted as random integers, then getting converted as key materials.

Saba *et al.* [34] proposed a blockchain methodology that is encrypted for supercomputing within the context of big data. To safeguard real-time activities associated with financial transactions by utilizing the services dynamically provided by the Software Defined Networks (SDN), the model was designed. Bag *et al.* [4] proposed a hardware micro-program technique that demonstrates reduced consumption of resources in comparison to existing technique in Field-Programmable Gate Array (FPGA), which offers improved programming flexibility. It employs redundant numerical arithmetic requires only 2×506 slices on the Xilinx Virtex-7FPGA. Saha *et al.* [35] offer a secure protocol utilizing ECC, designed to facilitate multicast and broadcast of Internet of Things (IoT) data. The

proposed communication protocol has been shown to perform well regarding computation overheads, along with functional features. Ren *et al.* [32] offers an efficient protocol for authentication asymmetric key management in LEO-terrestrial networks, incorporating ECC. This protocol mitigates the limitations identified in previous studies, significantly decreases the computational burden on client-server, and presents a novel methodology for the updating the session keys. This security evaluation for interacting necessitates the application of both formal and informal analytical techniques. Al-Khaleel *et al.* [3] offered a novel approach for IoT devices utilizing the FPGA-pair based ECC, characterized by their lightweight design and efficient behaviour. One ECC based processor operates in parallel, providing increased speed, whereas the other functions serially, resulting in a more compact design. Zhang *et al.* [42] implemented a novel authentication and key agreement system utilizing the physical function in conjunction with the chameleon function, demonstrating enhanced effectiveness. The overheads in gateway are maintained by the system at a controllable level, ensuring minimal impact on parties involved for authentication. The implementation of device anonymity is contingent upon basic operations such as hashing and XOR. A comprehensive security analysis was performed using the ProVerif tool, BAN logic, and the widely accepted real-or-random model. Kwon *et al.* [21] present a multi-domain authentication technique utilizing consortium blockchain to ensure safe and constructive V2G services, the protocol employs XOR operators and hash functions to facilitate lightweight intra domain authentication mechanism. This protocol ensures safe cross-domain authentication through the integration of ECC and Physical Unclonable Function (PUF) which can lead to increased confidence and enhance effective communication. Kenioua *et.al* [16] proposed a novel method of securely transmitting the signals for vehicle positioning of the autonomous vehicles. This approach is based on the leader control one, such that, the group of the vehicle will be operated based on the signals given by the leader. If the leader vehicle signal is hacked and the entire system gets collapsed.

Three approaches are employed to optimize the area-efficient hardware design introduced by Aljaedi *et al.* [2] for executing the elliptic-curve PM operation over $GF(2^{233})$: To perform multiplication of two polynomials with clock cycle overhead, the following steps are implemented:

1. A bit-serial-based booth polynomial multiplication architecture is utilized.
2. The arithmetic unit incorporates a single modular adder, booth multiplier, and square block.
3. The computation of modular inversion is achieved through the use of the implemented square and booth multiplier circuits.

3.2. Research gap in the Existing System

The literature presented in section 3.1, several problems and research gaps within the environment were identified. The ECC algorithm supports high confidentiality; however, ECDSA is needed for authentication, this entails high computational complexity. Therefore, it is necessary to modify ECC to decrease this computational complexity and enable authentication support. 3.2 An enhanced algorithm is required to effectively utilize the TLS protocol.

3.2.1. Elliptic Curve Cryptography Algorithm for Encryption but no Authentication

The public and private keys, along with the required other public parameters and the actual text message all to be encrypted, are specified as follows: Alice transmits a message to Bob.

- Encryption: $(C_1, C_2) = (P_m + kP_B), (kG)$ given that the message P_m is encrypted with Bob's public key, which is accessible to everyone, there is a lack of authentication to ensure that Alice is the one sending the message. However, we can achieve a high level of confidentiality, as k is the random number that is exclusively known to the sender.
- Decryption: $P_m = C_1 - n_B C_2 = P_m + kP_B - n_B kG = P_m + kn_B G - kn_B G = P_m$. Note that the message is decrypted by Bob with his own private key applied. Therefore, the current algorithm ensures confidentiality but fails in authentication.

3.2.2. Need of Cryptographic Algorithms for Efficient Utilization of Transport Layer Security

TLS is the highly secure encrypted protocol, which is operated at the higher layer of the TCP. It is designed to construct an encapsulated tunnel for securely transmit the sensitive information between two communicating parties, thereby preventing unauthorized access or eavesdropping by hackers or other malicious entities. The process of establishing a secure connection in the communication involves three distinct steps. The processes involved include the TCP handshake, verification of certificates, and exchange keys. The current implementation is TLS 1.3, which offers the fastest handshake process with a streamlined approach to certificate verification. During the key exchange phase, various algorithms are employed for specific functions, [1] such as RSA for ensuring confidentiality, ECDH for facilitating key exchange, and Message Authentication Code (MAC) for providing message authentication and integrity [22, 23]. These algorithms are essential for establishing a secure communication. Wang *et al.* [40] proposed a three-level implementation in TLS protocol to change from synchronous to asynchronous, but using the same existing cryptographic algorithms in three steps. Several vulnerabilities found in remote attestation

and attested TLS using the secure tool called ProVerif [40] due to the existing usage of the algorithm in three steps. The proposed algorithm is applicable to various security principles and by making it highly applicable for the TLS protocol compared to other algorithms currently in use.

4. Proposed Methodology

The overall process implemented for secure data transmission between Alice (sender) and Bob (receiver) using modified ECC algorithm is given in Figure 2. The plain text is considered as the message or data need to be securely transferred, and it should be converted into the elliptic curve points using CRT based ECC point conversion algorithm presented Menandas and Christo [25]. The detailed description of the modules represented in Figure 2 (rectangular box) are:

- Declaration of public parameters and key generation using CRT.
- Initial setup for authentication.
- Modified elliptic curve encryption.
- Authentication and integrity check.

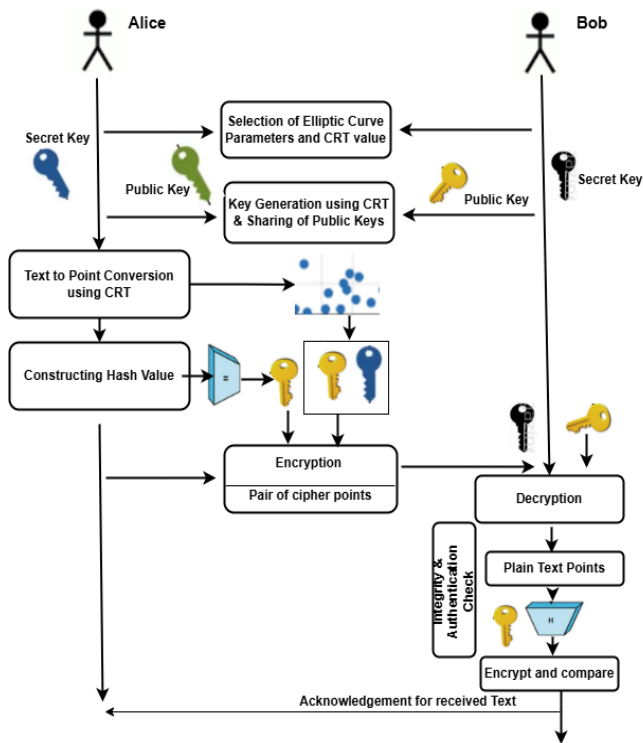


Figure 2. The overall architecture for secure data transmission using modified ECC algorithm.

4.1. Public Parameters Declaration and Generating Key Pair

Select the elliptic curve $E_p(a, b)$ from Equation (2) $y^2 = x^3 + ax + d$, where x, y, a, b are real numbers, and the values of a, b should satisfy the Equation (4) $a^3 + 27b^2 \mod p \neq 0$, also choose the generator point of elliptic curve $G(x, y)$ such that, the order of the curve should be maximum. Therefore, the public parameters are, $E_p(a,$

$b), G(x, y)$.

Each identity involving the communication must do

1. Choose n_A be the very larger value.
2. Choose the CRT value C_A such that which can be large enough and possibly of two prime moduli. Let $C_A = M_1 \times M_2$.
3. Calculate $K_{A1} = n_A \mod M_1, K_{A2} = n_A \mod M_2$
4. Calculate public key $KA_{pub} = K_{A1} \cdot G \cdot K_{A2} \cdot G$
5. Private key $KA_{pri} = K_{A1} + K_{A2}$
6. To keep KA_{pri} as private key and distribute KA_{pub} to communicating parties.

Step 1 to 6 are the key generation for Alice (say A for sender), the same steps done by all communicating parties involving it.

4.2. Initial Setup for Integrity and Authentication

The integrity is used to prove the correctness of the message/data ensure that the transferred message is not altered under any cause. Hash algorithms are involved to prove the identity of the transferred information. Here we used a simple hash algorithm called SHA-256, which calculates a fixed length message digest irrespective of the length of the message. In our proposed algorithm, hash value is directly calculated from the original plain text, and encrypted hash value separately by senders public key, and message along with the hash value is again encrypted by receivers public key and senders private key to obtain confidentiality,

4.3. Modified Elliptic Curve Encryption

The message needs to be transferred to the receiver to be converted into EC $E_p(a, b)$ of points, using CRT [25].

Let P_m be the message, represented as a set of characters, $P_m = (P_{m1}, P_{m2}, \dots, P_{mn})$, for every $P_{mi} \in P_m$ to be converted into point $P_i(x, y)$ and hence.

$$P(x, y) = (P_1(x, y), P_2(x, y), \dots, P_n(x, y)) \leftrightarrow P_m = (P_{m1}, P_{m2}, \dots, P_{mn})$$

$\forall P_i(x, y)$ do:

1. Calculate $H(m_i) \leftarrow \text{Hash}(P_{mi})$
2. Calculate $T_1 = KA_{pri} \times H(m_i)$ //an integer
3. Calculate $T_1(x, y) = T_1 \times KB_{pub}$ //point
4. Calculate $C_1(x, y) = P_i(x, y) + T_1(x, y)$
5. Calculate $T_2(x, y) = KA_{pub} \times H(m_i)$ //point
6. Calculate $C_2(x, y) = T_2(x, y)$

Hence the calculated cipher text point,

$$P_i(x, y) \rightarrow (C_{i1}(x, y), C_{i2}(x, y))$$

4.4. Modified Elliptic Curve Decryption

The cipher text pair (C_1, C_2) , first to extract the key to get

plain text from C_2 by multiplying the receivers private key then subtract the result from C_1 . For each $(C_{i1}(x, y), C_{i2}(x, y))$ do:

1. Compute $T_1 = KB_{pri} \times C_{i2}(x, y)$
2. Compute $P_i(x, y) = C_{i1}(x, y) - T_1$

The formal proof of getting the plain text as follows,

$$\begin{aligned} P_i(x, y) &= C_{i1}(x, y) - KB_{pri} \times C_{i2}(x, y) = P_i(x, y) + KA_{pri} \times H(m_i) \times KB_{pub} - KB_{pri} \times C_{i2}(x, y) \\ &= P_i(x, y) + KA_{pri} \times H(m_i) \times KB_{pub} - KB_{pri} \times KA_{pub} \times H(m_i) = P_i(x, y) + (KA_1 + KA_2) \times H(m_i) \times (KB_1 + KB_2) \times G \\ &\quad - (KB_1 + KB_2) \times (KA_1 + KA_2) \times G \times H(m_i) = P_i(x, y) + (KA_1 + KA_2) \times (KB_1 + KB_2) \times G \times H(m_i) \\ &\quad - (KB_1 + KB_2) \times (KA_1 + KA_2) \times G \times H(m_i) = P_i(x, y) \end{aligned}$$

4.5. Authentication and Integrity Check

After the decryption of the message, the integrity of the message is evaluated to ensure that the received message is not changed during transmission. The checking of authentication and integrity as follows,

1. Calculate $H(m) \leftarrow \text{Hash}(m)$
2. Calculate $H(m) \times KA_{pub} \leftrightarrow (x'_{c2}, y'_{c2}) = H(m) \times (x_{KA_{pub}}, y_{KA_{pub}})$
3. Verify that $x_{c2} = x'_{c2}$ and $y_{c2} = y'_{c2}$ for proving integrity.

The pictorial presentation of proving authentication and integrity is given in Figure 3. It includes the actual decryption given in section 4.4. After getting the

plaintext, the same hash algorithm applied to get the message digest and encrypt with senders public key then verify with the second part of the received cipher text.

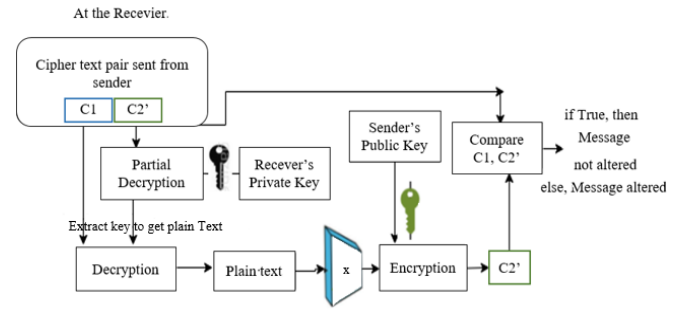


Figure 3. Authentication and integrity check after decryption process by the receiver.

Figure 4 shows the utility of modified ECC in connection establishment of TLS/SSL. After the connection establishment, checking certificate, key exchange and data transmission are done by the same modified ECC proposed algorithm with reduced steps. Also the same algorithm will support confidentiality, integrity and authentication which all needed in TLS/SSL protocol.

The existing protocol uses the session key (symmetric key) for secure data transmission, instead we can use the pair of key for authentication and integrity.

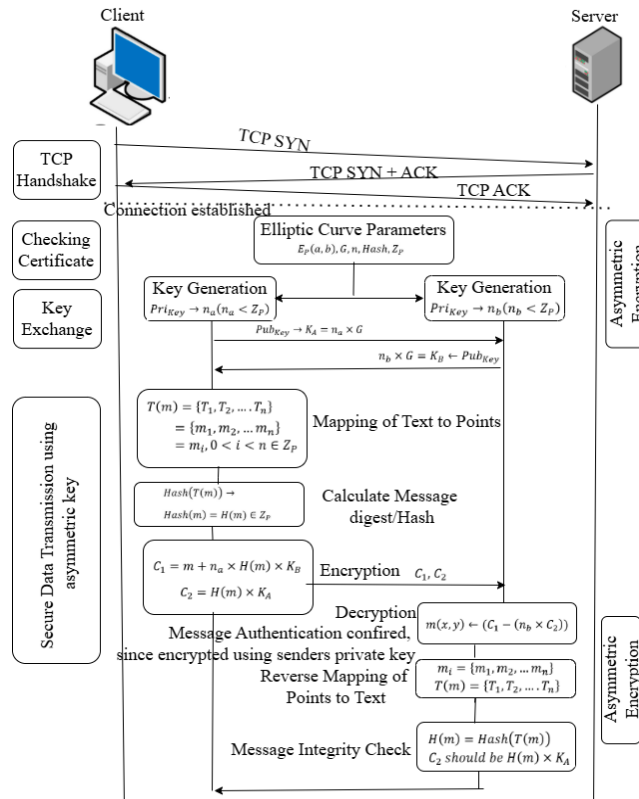


Figure 4. Flow diagram of connection establishment in TLS/SSL using modified ECC algorithm

4.6. Implementation of Key Generation in Modified ECC using CRT

The strength of the ECC mainly depends on the discrete

logarithmic problem, such that the selection of the single variable n_a should be very large, and the prime factor of the elliptic curve $E_p(a, b)$ also very large. To manipulate

the ECC algorithm with large numbers gives more complex, hence the utility is low in day today applications. To increase the utility of ECC, we introduced CRT, to process the larger numbers in an easy and efficient manner. That is reducing the larger value to the smaller one, based on the selected Chinese theorem value (C_i), process with smaller numbers and bring back the original value. With this time complexity is reduced and strength of the algorithm getting increased.

Also, there are several methods of doing point arithmetic with reduced loops, here we choose double and add method for performing point arithmetic (scaling). By combining the CRT and double and add method, we can highly reduce the number of loops, with the parallel execution of Chinese remainder two prime moduli.

The implementation is as follows,

1. Let n_a be the larger value selected as secret, and based

on the C_a it is converted into smaller value like:

$M_1 = n_a \bmod m_1, M_2 = n_a \bmod m_2$ where

$C_a = m_1 \times m_2$ and $M_1, M_2 < n_a$, the private key is $(M_1 + M_2)$ and public key is $(M_1 G + M_2 G)$.

2. Convert M_1, M_2 in to binary $\rightarrow (M_1)_2, (M_2)_2$.
3. Find the common prefix of $(M_1)_2$ and $(M_2)_2$.
Let it be Com-Prefix $((M_1)_2$ and $(M_2)_2$).
4. Now apply double and add method, leave the first digit of Com-Prefix $((M_1)_2$ and $(M_2)_2$).
5. Set result = G .
6. for every digit(i) do
If $i=1$ then, result = point-double (result),
result = result + G
Else result = point-double(result)
7. Continue remaining digits of $((M_1)_2$ and $(M_2)_2$) separately.

Figure 5 shows the implementation with sample number.

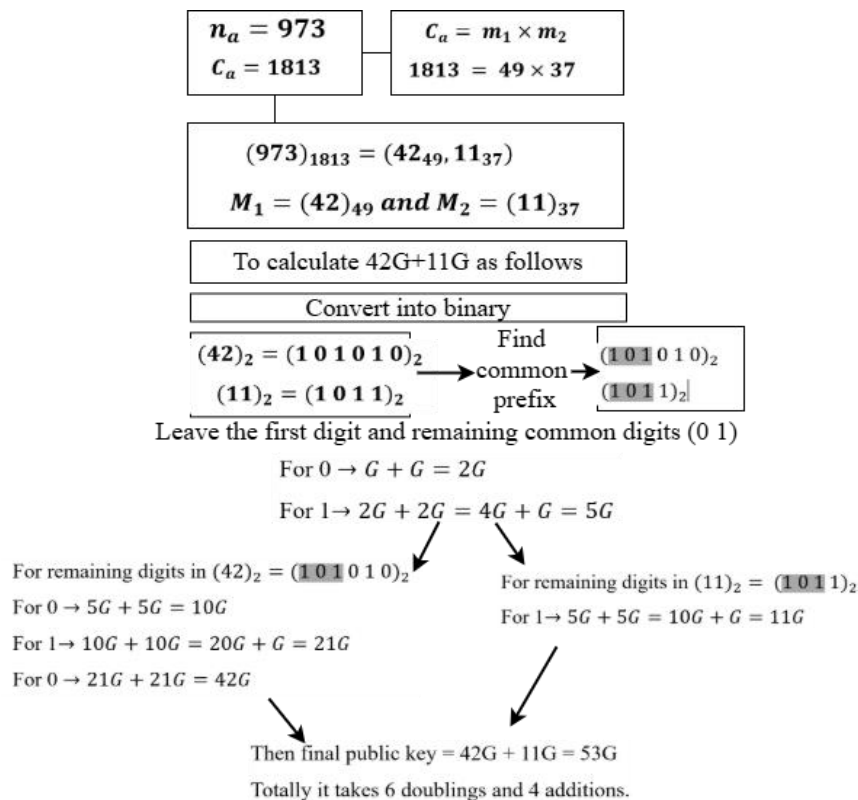


Figure 5. Simple example for generating keys using CRT and double and add method.

5. Execution and Performance Analysis

The performance of the proposed algorithm analysed with the simple database application (bio-data of medical card). The front end is implemented with python, and the Microsoft excel is used as the database storage. The implementation is being conducted using sublime text version-3 on a Lenovo think book laptop model equipped with an Intel CORE i5 processor running at 2.20 GHz and 16 GB of RAM. The system utilizes a 192-bit key size as per the recommendations of National Institute of Standards and Technology (NIST) for Elliptic curve parameter implementation. This setup

ensures optimal performance and compliance with industry standards for secure cryptographic operations.

5.1. Sample Input and Output

Figure 6 shows the input to modified ECC algorithm, contains the patient details. When we save the patient details, it is converted into the cipher text, and stored in the database. The format of the database after pressing SAVE button is given in Figure 7. That is the size of every field is very large, as shown the first name itself alone. For remaining fields of the first part of the cipher text alone is given in Figure 7.

Patient Demographics

First Name	Ellice	Last Name	Vinnay		
Sex	Female	DOB	01/01/1992		
Address	No:4, Maurice Steet
Calalpet, Chennai		Phone		9444123456
			Occupation		Teaching

Patient Unique ID	Blood Group	Drug Allergy	Health Insurance ID	Health Insurance Company
EV56153R	O -	Ibuprofin,
Asperin	XYZ123	Star_XYZ, Chennai

Referring Doctor	Hospital Name	Date and Time of Visit
Dr.Innocent	St.Thomas Hospitals,
Chennai	01/03.2023: 10:33

Patient Present Health Details			Prescription Paracetamol (3)
Naproxen (3)
Cefadroxil(3)	
Temperature	100 F	Glycemia		120
Hypertension	140/100	eAG		110
		Oxygen Saturation		98

Figure 6. Sample input (we have taken a simple database application-medical card details).

First name																				
2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 6193199055113969152687712056392098586164011469																				
Last name																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 1093359880438658879574289644868084444394609																				
Sex																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Address																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 23554770375276393963212126734477114459696504																				
DOB																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 239218155544474340746898100298016306657533633																				
Phone																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Occupation																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 510317736571575959206430813413893058969062918																				
Patient_Unique_ID																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 1093359880438658879574289644868084444394609																				
Drug Allergy																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 108935472392687523018043704324165410367112034																				
Health Insurance Company																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Health Insurance ID																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 287801859439084267729938074161718502302116046																				
Referring Doctor																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Hospital Name																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Date of Visit																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 239218155544474340746898100298016306657533633																				
Client_Health_Details																				
Temperature																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 108935472392687523018043704324165410367112034																				
Hyper Tension																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 108935472392687523018043704324165410367112034																				
Glycemia																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 108935472392687523018043704324165410367112034																				
Oxygen Saturation																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 465051747881833432256989649046804483171904672																				
Heart Rate																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 1093390791727336090078995058382866101153531347																				
eAG																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 108935472392687523018043704324165410367112034																				
Prescription																				
[2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426, 1093390791727336090078995058382866101153531347																				

Figure 7. Database contents after encryption.

Patient Demographics:

1. First name: Ellice
2. Last name: Vinncy
3. Sex: Female
4. DOB: 01/01/1992
5. Address: No:4, Maurice Street Calalpet, Chennai
6. Phone: 9444123456
7. Occupation: Teaching
8. Patient_Unique_ID: EV56153R
9. Blood Group: O-
10. Drug Allergy: Ibuprofen, Asperin
11. Health_Insurance_Company: Star_XYZ, Chennai
12. Health_Insurance_ID: XYZ123
13. Referring Doctor: Dr. Innocent
14. Hospital_Name: St. Thomas Hospital, Chennai
15. Date of Visit: 01/03/2023: 10:33
16. Patient_Health_Details
17. Temperature: 100 F
18. Blood Pressure: 140/100
19. Glycemia: 120
20. eAG: 110
21. Heart Rate: 60
22. Oxygen Saturation: 98
23. Prescription: Paracetamol (3), Naproxen (3), Cefadroxil (3)

Figure 8. Getting original text after decryption.

To view the patient report, by decrypting the encrypted details using patients' private key, after decryption the report is generated and shown in Figure 8. The given plain text called patient demographics, is initially converted into corresponds ASCII values. These ASCII values are represented in CRT. After encryption, the plain text points are transformed into cipher text points, which are then decrypted back to the original plain text points. Thus, the encryption and decryption process successfully preserve the integrity of the plain text message. The obtained values correspond to the selected Generator value, if the generator value changed and the input text remains the same, the cipher text varies accordingly. Similarly, different values yield distinct cipher texts. These cipher texts are then transmitted to the receiver for decryption and further processing. The implementation demonstrates the robustness and

scalability of modified ECC for securing communications in resource-constrained environments, such as IoT-enabled healthcare systems. The use of smart cards and efficient cryptographic algorithms ensures the confidentiality and integrity of sensitive patient data transmitted over the network.

5.2. Computational Complexity of Proposed Algorithm

The computational complexity of proposed modified ECC algorithm is shown in Table 2. The length of elliptic curve prime value is 58, the length of the input pain text is 24, and the chosen CRT value is as large as possible and closer the largest elliptic curve point. The modified ECC algorithm is executed with the above said information module by module and repeatedly. The average time is taken in (μ s) for every module and given in Table 2. It shows that, the overall time taken for CRT and double and add method is very less when compared to other algorithms.

Table 2. The computational complexity of the individual module of proposed ECC algorithm.

Name of the module	Curve points in numbers	Points to be processed in numbers	Time taken w/o CRT (μ s)	Time taken with CRT (μ s)	Time with CRT and double and add (μ s)
Text to points	24	48	800	300	250
Encryption	48	49	3200	1300	1100
Decryption	49	48	3500	1500	1400
Point to text	48	24	950	700	550
Integrity check	24	48	2900	1400	1200

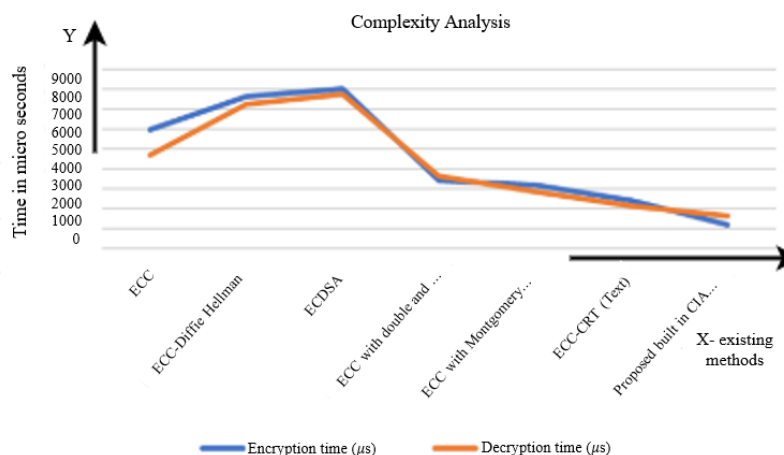


Figure 9. Time complexity of ECC based algorithms.

Table 3. The time complexity of modified ECC with existing ECC based algorithms.

Elliptic cubic curve algorithms	Encryption in μ s	Decryption in μ s
ECDSA	8100	7730
ECC	5850	4780
Diffie Hellman	7500	7310
ECC-montgomery ladder	3250	2860
ECC-double and add	3440	3650
ECC-CRT (text)	2400	2100
Modified ECC-CRT double and add	1210	1500

The overall encryption and decryption time of ECC based algorithms shown in Table 3, and the complexity analysis compared with existing ECC based algorithm with modifies ECC algorithm. In general the PM performed with double and add method reduce the execution time. But when the CRT method incorporated with the double and add method will drastically reduce the execution time. The Figure 9 shows the graph diagram for comparing the encryption and decryption

time of ECC based algorithm and modified ECC algorithm.

5.3. Security Strength

The security calculation comparison outcome of symmetric and asymmetric cryptographic methods based on selected key size is displayed in Table 4. ECC offers robust security with a short key length, as researchers have already demonstrated. However, it doesn't offer integrity checks or authentication. Authentication and integrity are demonstrated in our suggested approach, making it extremely safe.

Table 4. Strength of modified-ECC with variable key length.

Symmetric cryptography	Asymmetric cryptography (keys in bits)			
	RSA	ECC and ECDSA	Built-in CIA-ECC	ECC-CRT based double and add
80	1024	160	160	128
112	2048	224	192	160
128	3072	256	224	192
192	7680	384	256	224

Figure 10 shows the security strength of modified ECC with other algorithms with respect to different key size. As we know that, RSA provides strong security for larger key size, at the same time ECC based algorithms gives similar security strength with small key size. In Figure 11 we shows the security strength of only ECC based algorithms with different key size. In Figures 10

and 11, X-axis represents the algorithm, and Y-axis represents the variable key sizes. In the graph series in different colors indicate that the strength we obtain for the specific algorithm corresponds to the key size.

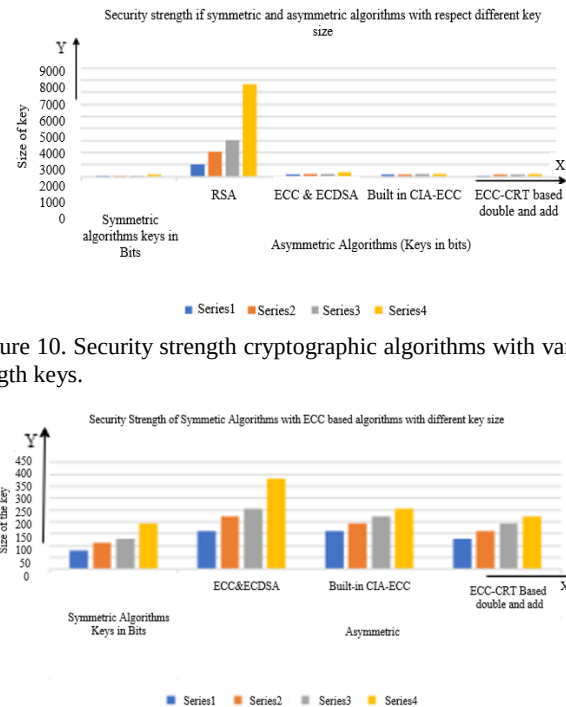


Figure 10. Security strength cryptographic algorithms with variable length keys.

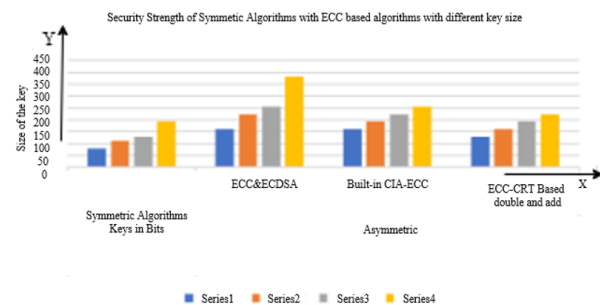


Figure 11. Security strength comparison with ECC based algorithms with variable key size.

Table 5. Security services of ECC-CRT with other algorithms.

Asymmetric cryptographic algorithms	Security services				
	Data confidentiality	Access control	Authentication	Non-repudiation	Data integrity
RSA	✓	✓	✓	✓	✓
Diffie-Helman		✓	✓		✓
ECC	✓	✓			
ECDSA		✓	✓	✓	✓
CRT-ECC	✓	✓	✓	✓	✓

Regarding security service aspects Table 5, compares the performance of the suggested (ECC-CRT) with existing asymmetric algorithms. Even though RSA integrated with all security aspects, but after the invention of Shor's algorithm for finding prime factorization problem, increase serious threats of breaking RSA. The overall security strength of ECC algorithm is very high when compared to that of RSA, also breaking of the discrete logarithmic problem is highly hard to compared that of prime factorization problem. The overall security services are supported only in the modified ECC with CRT, because, the ECC does not support authentication because of random number is used for encryption, also not support data integrity and non-repudiation, also ECDSA do not support confidentiality. Hence our proposed algorithm ECC-CRT only support all security parameters.

5.4. Security Threat-Side Channel Attack

Threats and assaults against edge devices, such as sensor nodes, are the primary emphasis of the WSN. These nodes must be resistant to threats or attacks due to their

extremely low resource use [14]. Devices that use the elliptic curve method are located distant from known security risks associated with the applications. However, it also requires additional defence against Side Channel Attacks (SCA) like timing and Power Analysis Attacks (PAA). Let's see how the sensor nodes are shielded from these attacks by our suggested approach.

5.4.1. Side Channel Attack

It always learn from the side channel information analysis and trying to find the possible secret information and inner working of the algorithm. The side channel analysis contains the information about running time of the algorithm based on the length of the input bits to the generated output, power consumption by the processor with respect to the hardware used for different input, amount of electromagnetic radiation, and sound functions. The timing attack and power analysis attack constitutes to be the SCA.

5.4.2. Timing Attack

Timing attack is performed by calculating amount of

time required for elliptic curve point arithmetic, and secure key generations with the respective length. In general, the point arithmetic is performed based on the bit pattern. Our suggested method divides the input according to the value of CRT, allowing for key generation, encryption, and decryption to be performed without relying on random values. Instead, it utilizes the message digest of each input. Consequently, there is no chance for attackers to learn the time required to generate keys, which means our proposed ECC-CRT is immune to timing attacks.

5.4.3. Power Analysis Attack

The power analysis attack is performed by learning the Central Processing Unit (CPU) power traces, CPU electromagnetic radiation and some physical observables like various execution time, various power consumption and enforced unexpected behaviors. The primary implementation of the ECC algorithm is based solely on point arithmetic operation. And the study demonstrated that a PAA is extremely feasible in ECC based algorithms because, the point arithmetic operation is executed in a linearly [14]. The objective is to execute nG for the specified values of n and point G , through a loop that iterates 1 to n . Our proposed ECC-CRT utilizes point arithmetic through CRT with the double and add method, resulting in varying running times even for identical CRT and G values, thereby preventing any key information from being extracted via PAA. Thus, through the process of converting text to points and conducting integrity checks, we have implemented the CRT using the double and add method. Consequently, we assert that our recommended algorithm is resistant to PAA.

6. Conclusions and Future Work

Our suggested method is a modified ECC-CRT algorithm for secure use in WSN devices integrating with all security mechanisms in a single step. We demonstrated that our algorithm is devoid of security threats such as side channel and PAA by implementing point arithmetic through a combination of CRT and the double and add method. Also, provides the reduced time complexity and strong security even for less key length. By the performance comparison our proposed algorithm is the best one to reduce the running time utilized in TLS/SSL protocol of WSN.

Future considerations for small scale sensor devices must include threats posed by quantum computation. In future the novel cryptographic methods require to protect ECC based algorithms against post quantum computation.

References

- [1] Ahmadi K., Aghapour S., Kermani M., and Azarderakhsh R., "Efficient Error Detection Cryptographic Architectures Benchmarked on FPGAs for Montgomery Ladder," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 32, no. 11, pp. 2154-2158, 2024. DOI:10.1109/TVLSI.2024.3419700
- [2] Aljaedi A., Qureshi F., Hazzazi M., Imran M., Bassfar Z., and Jamal S., "FPGA Implementation of Elliptic-Curve Point Multiplication over GF(2^{233}) Using Booth Polynomial Multiplier for Area-Sensitive Applications," *IEEE Access*, vol. 12, pp. 72847-72859, 2024. DOI:10.1109/ACCESS.2024.3403771
- [3] Al-Khaleel O., Baktir S., and Kupcu A., "Efficient ECC Processor Designs for IoT Using Edwards Curves and Exploiting FPGA Embedded Components," *IEEE Access*, vol. 12, pp. 167183-167200, 2024. DOI:10.1109/ACCESS.2024.3495995
- [4] Bag A., Roy D., Patranabis S., and Mukhopadhyay D., "FlexiPair: An Automated Programmable Framework for Pairing Cryptosystems," *IEEE Transactions on Computers*, vol. 71, no. 3, pp. 506-519, 2022. DOI:10.1109/TC.2021.3058345
- [5] Chen Y., Yin F., Hu S., Sun L., Li Y., and Xing B., "ECC-Based Authenticated Key Agreement Protocol for Industrial Control System," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 4688-4697, 2023. DOI:10.1109/JIOT.2022.3219233
- [6] Cohen H., Frey G., Avanzi R., Doche C., Lange T., Nguyen K., and Vercauteren F., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman and Hall/CRC, 2012. <https://sites.cs.ucsb.edu/~koclab/teaching/ccs130/h/2013/EllipticHyperelliptic-CohenFrey.pdf>
- [7] Dabholkar A. and Yow K., "Efficient Implementation of Elliptic Curve Cryptography (ECC) for Personal Digital Assistants (PDAs)," *Wireless Personal Communications*, vol. 29, pp. 233-246, 2004. <https://doi.org/10.1023/B:WIRE.0000047066.74117.86>
- [8] Dimitrov V. and Cooklev T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 78, no. 1, pp. 82-87, 1995. https://globals.ieice.org/en_transactions/fundamentals/10.1587/e78-a_1_82/_p
- [9] Ding C., Pei D., and Salomaa A., *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific, 1996. <https://books.google.jo/books?id=RQLtCgAAQB AJ>
- [10] Gallant R., Lambert R., and Vanstone S., "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms," in *Proceedings of the Advances in Cryptology Conference*, Santa

- Barbara, pp. 190-200, 2001. <https://doi.org/10.1007/3-540-44647-8>
- [11] Guzey S., Kurt G., and Ozdemir E., "Group Authentication and Key Establishment Scheme," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 35086-35099, 2024. DOI: 10.1109/IIOT.2024.3436652
- [12] Han Y., Guo H., Liu J., Ehui B., Wu Y., and Li S., "An Enhanced Multifactor Authentication and Key Agreement Protocol in Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16243-16254, 2024. DOI:10.1109/IIOT.2024.3355228
- [13] Hankerson D., Vanstone S., and Menezes A., *Guide to Elliptic Curve Cryptography*, Springer, 2006. <https://doi.org/10.1007/b97644>
- [14] Houssain H., Badra M., and Al-Somani T., "Power Analysis Attacks on ECC: A Major Security Threat," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 6, pp. 90-96, 2012. <http://dx.doi.org/10.14569/IJACSA.2012.030615>
- [15] Joye M. and Yen S., "The Montgomery Powering Ladder," in *Proceedings of the Cryptographic Hardware and Embedded Systems Conference*, Cologne, pp. 291-302, 2003. https://doi.org/10.1007/3-540-36400-5_22
- [16] Kenioua L., Lejdel B., and Nedioui M., "A Comprehensive Approach to Combat GPS Spoofing and Ensure Security Positioning in Autonomous Vehicles," *The International Arab Journal of Information Technology*, vol. 21, no. 4, pp. 627-635, 2024. <https://doi.org/10.34028/iajit/21/4/7>
- [17] Kibler M., *Galois Fields and Galois Rings Made Easy*, Elsevier Ltd, 2017. <https://doi.org/10.1016/C2016-0-01243-3>
- [18] Koblitz N., "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987. <https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/>
- [19] Koblitz N., Menezes A., and Vanstone S., "The State of Elliptic Curve Cryptography," *Designs, Codes and Cryptography*, vol. 19, pp. 173-193, 2000. <https://doi.org/10.1023/A:1008354106356>
- [20] Kwon D., Son S., Kim M., Lee J., Das A., and Park Y., "A Secure Self-Certified Broadcast Authentication Protocol for Intelligent Transportation Systems in UAV-Assisted Mobile Edge Computing Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 19004-19017, 2024. DOI: 10.1109/TITS.2024.3428491
- [21] Kwon D., Son S., Park K., Das A., and Park Y., "Design of Blockchain-Based Multi-Domain Authentication Protocol for Secure EV Charging Services in V2G Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 12, pp. 21783-21795, 2024. DOI:10.1109/TITS.2024.3472013
- [22] Lan X., Xu J., Zhang Z., and Zhu W., "Investigating the Multi-Ciphersuite and Backwards-Compatibility Security of the Upcoming TLS 1.3," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 272-286, 2019. DOI:10.1109/TDSC.2017.2685382
- [23] Li P., Su J., and Wang X., "iTLS: Lightweight Transport-Layer Security Protocol for IoT with Minimal Latency and Perfect Forward Secrecy," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6828-6841, 2020. DOI:10.1109/IIOT.2020.2988126
- [24] Li X., Niu J., Bhuiyan M., Wu F., Karuppiah M., and Kumari S., "A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599-3609, 2018. DOI:10.1109/TII.2017.2773666
- [25] Menandas J. and Christo M., "Chinese Remainder Theorem-Based Encoding of Text to Point Elliptic Curve Cryptography," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 47, no. 2, pp. 148-159, 2025. <https://doi.org/10.37934/araset.47.2.148159>
- [26] Miller V., "Use of Elliptic Curves in Cryptography," in *Proceedings of the Theory and Application of Cryptographic Techniques Conference*, Santa Barbara, pp. 417-426, 1985. https://doi.org/10.1007/3-540-39799-X_31
- [27] Mohamed N., Hashim M., and Hutter M., "Improved Fixed-Base Comb Method for Fast Scalar Multiplication," in *Proceedings of the International Conference on Cryptology in Africa*, Morocco, pp. 342-359, 2012. https://doi.org/10.1007/978-3-642-31410-0_21
- [28] Oladipupo E., Abikoye O., Imoize A., Awotunde J., Chang T., and Lee C., "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks," *IEEE Access*, vol. 11, pp. 1306-1323, 2023. DOI: 10.1109/ACCESS.2022.3233632
- [29] Puckett S., Liu J., Yoo S., and Morris T., "A Secure and Efficient Protocol for LoRa Using Cryptographic Hardware Accelerators," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22143-22152, 2023. DOI:10.1109/IIOT.2023.3304175
- [30] Rabah K., "Theory and Implementations of Elliptic Curve Cryptography," *Journal of Applied Sciences*, vol. 5, no. 4, pp. 604-633, 2005. DOI: 10.3923/jas.2005.604.633
- [31] Rafique F., Obaidat M., Mahmood K., Ayub M., Ferzund J., and Chaudhry C., "An Efficient and

- Provably Secure Certificateless Protocol for Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8039-8046, 2022. DOI:10.1109/TII.2022.3156629
- [32] Ren S., Liu J., Ji R., Ge S., and Li D., “A Secure Authentication Scheme for Satellite-Terrestrial Networks,” *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 6, pp. 6470-6482, 2024. DOI:10.1109/TNSE.2024.3445712
- [33] Rivest R., Shamir A., and Adleman L., “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978. <https://doi.org/10.1145/359340.359342>
- [34] Saba T., Haseeb K., Rehman A., and Jeon G., “Blockchain-Enabled Intelligent IoT Protocol for High-Performance and Secured Big Financial Data Transaction,” *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1667-1674, 2024. DOI:10.1109/TCSS.2023.3268592
- [35] Saha K., Ray S., and Dasgupta M., “ECMHP: ECC-Based Secure Handshake Protocol for Multicasting in CCN-IoT Environment,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5826-5842, 2024. DOI:10.1109/TNSM.2024.3419431
- [36] Seo H., Kim H., Park T., Lee Y., Liu Z., and Kim H., “Fixed-Base Comb with Window-Non-Adjacent Form (NAF) Method for Scalar Multiplication,” *Sensors*, vol. 13, pp. 9483-9512, 2013. DOI:10.3390/s130709483
- [37] Shuai M., Xiong L., Wang C., and Yu N., “A Secure Authentication Scheme with Forward Secrecy for Industrial Internet of Things Using Rabin Cryptosystem,” *Computer Communications*, vol. 160, pp. 215-227, 2020. <https://doi.org/10.1016/j.comcom.2020.06.012>
- [38] Tsaur W. and Chou C., “Efficient Algorithm for Speeding up the Computations of Elliptic Curve Cryptosystem,” *Applied Mathematics and Computation*, vol. 168, no. 2, pp. 1045-1064, 2005. <https://doi.org/10.1016/j.amc.2004.10.010>
- [39] Viswanathan S. and Kannan A., “Elliptic Key Cryptography with Beta Gamma Functions for Secure Routing in Wireless Sensor Networks,” *Journal of Mobile Communication, Computation and Information*, vol. 25, pp. 4903-4914, 2019. <https://doi.org/10.1007/s11276-019-02073-9>
- [40] Wang Y., Gamage T., and Hauser C., “Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication,” *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 807-816, 2016. DOI:10.1109/TSG.2015.2499766
- [41] Wu F., Li X., Xu L., Vijayakumar P., and Kumar N., “A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120-1129, 2021. DOI:10.1109/JSYST.2020.2981049
- [42] Zhang Q., Zhou X., Zhong H., Cui J., Li J., and He D., “Device-Side Lightweight Mutual Authentication and Key Agreement Scheme Based on Chameleon Hashing for Industrial Internet of Things,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7895-7907, 2024. DOI:10.1109/TIFS.2024.3451357
- [43] Zhang Y., Li B., Wu J., Liu B., Chen R., and Chang J., “Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT,” *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22501-22515, 2022. DOI:10.1109/JIOT.2022.3176192



Josepha Menandas received a Bachelor of Engineering and Computer Science degree from Manonmaniyam Sundaranar University. She obtained a Master of Engineering and Computer Science degree from Sathyabama University in Chennai. She has taught for over 13 years, and she is presently pursuing a Ph.D. in Algorithm Analysis and Cryptographic Algorithms at SRM Institute of Science and Technology in Chennai. Algorithm Analysis, Network Security, and Machine Learning are among her areas of interest.



Mary Subaja is obtained BE in Computer Science and Engineering from St.Xavier's Catholic College of Engineering. Also holds an M.Tech in Information Technology from Sathyabama University, Chennai, and Ph.D. in the Specialization of Network security in Sathyabama University, Chennai. She has published 22 papers in various international journals, published 2 books, and 3 patents. She is working as an Associate Professor in the Department of Computer Science and Engineering School of Computing in SRMIST (SRM University), Kattankulathur, Chennai, India. Her research interests include but not limited to; Computer Networks, Wireless Communications, WSNs, IoT, Machine Learning, Block Chain Technology.