EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 2, Article Number 5659
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A New Septupling Point 7P Arithmetic Formula for López-Dahab Coordinate and Affine Over Binary Elliptic Curve Cryptosystem

Waleed K. Abdulraheem

Department of Information System and Network, The World Islamic Sciences and Education University, Amman, Jordan

Abstract. The Elliptic Curve Cryptography (ECC) is one of the most prominent Asymmetric-based cryptosystems as it affords a higher level of security with small keys. According to National Institute of Standards and Technology (NIST), ECC gains the smallest secure key over the binary curve. In literature, the best field over binary curves is Lopez-Dahab (LD) and Affine coordinates, and it considered fit for lightweight cryptography in resource-constrained devices such as Internet of Things (IoTs). ECC consists of three operational levels; scalar multiplication, point arithmetic and field arithmetic. This research focuses on point arithmetic precomputation useful in scalar multiplication and then for field arithmetic. There is no existing formula for Septupling point $7P$ over binary curves in LD and Affine coordinates. A new precomputed Septupling point $7P$ is introduced in this paper using LD and non-supersingular affine coordinate over the binary field $E(\mathbb{F}_{2^m})$. This paper uses the form $7P = 2(3P) + P$, consisting of Doubling point, Tripling point and the point addition. Also, the form $2(3P)$ means the Sixtupling point is also proposed. Results show that the $7P$ is characterized by a cost of 19 $S + 28$ M, while the cost of Sixtupling point $6P$ is 14 $S + 19$ M. The point is mathematically proved as valid. The proposed point can be implemented for different scalar multiplication such as $w-NAF$ for $w = 4$, and multi-based scalar such as {2, 3, 7}-based scalar multiplication method.

2020 Mathematics Subject Classifications: 94A60, 11T71, 14G50, 68P25

Key Words and Phrases: Elliptic Curve Cryptography, Information Security, Binary curves, Affine coordinates, Point Septupling Arithmetic, Lightweight Cryptography

1. Introduction

Recently, Information security has become one of the most important research topics affecting, organizations, countries [1]. Cryptography is considered the most fundamental method used to ensure the information and cyber security [2]. As a mechanism for achieving security , cryptography is vital to protect our data, information, and communication from threats, intruders, and attackers [3]. Cryptography codes the information to ensure

DOI: https://doi.org/10.29020/nybg.ejpam.v18i2.5659

Email address: waleed.amin@wise.edu.jo (W. K. Abdulraheem)

the main three security services which are confidentiality, integrity and authenticity, [4], [5], and [6] as shown in Fig. 1. Confidentiality ensures the data is secret, integrity ensures that the data is not changed, while authentication verifies the message origin [7], [8] and [9].

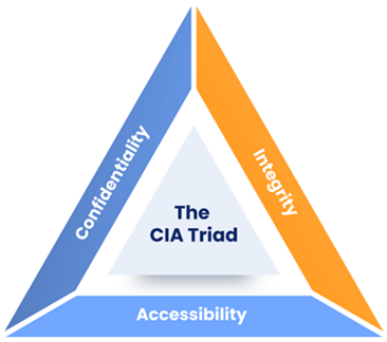

Figure 1: C.I.A Triad [7]

Cryptography can be divided into three types; symmetric, Asymmetric, and hashing algorithms [10] and [11]. According to national institute of standards and technology NIST, Symmetric key cryptography or private key refers to cryptographic algorithms that uses the same key for encryption and decryption operation, while Asymmetric or public cryptography refers to algorithms that uses two different keys to exchange information, one to digital sign or encrypt information and the other to decrypt it or to verify the digital signature [12] and [13] as in Fig. 2.

Although symmetric cryptosystems are very effective with respect to consumed time and resources, they still suffer from inherent problems in key distribution through the unsecure channels [14] and [15]. Asymmetric cryptosystem mechanisms facilitate key distribution over unsecure channels which assures both confidentiality and non-repudiation, however, the performance expectations are lower compared to symmetric cryptosystem [16] and [17].

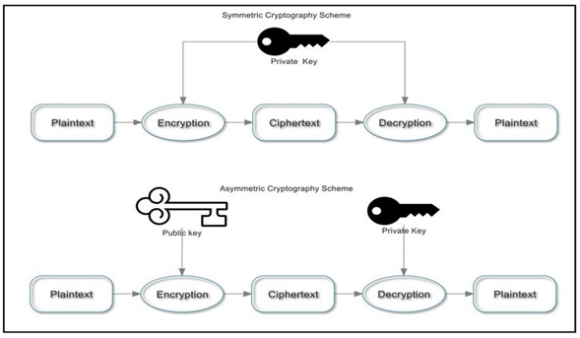

Figure 2: Symmetric and Asymmetric cryptosystems [18]

Elliptic curve cryptography ECC is a public key cryptosystem which has recently gained higher acceptance and popularity within the research community. This is because it achieves a significantly higher security level using short keys compared to other asymmetric cryptosystems [19] and [20]. As in Fig. 3, the ECC scalar multiplication is composed of three computational levels; scalar arithmetic, point arithmetic and finally field arithmetic. Scalar multiplication is to find the result of the operation $Q = kP$ such that $k \in N$, P *and* Q are two points on the curve. On the other hand, point arithmetic is adding two points on the curve $P + Q$ or $P + P$ (for point doubling). Field arithmetic are related to coordinates where the point operations are performed [21].

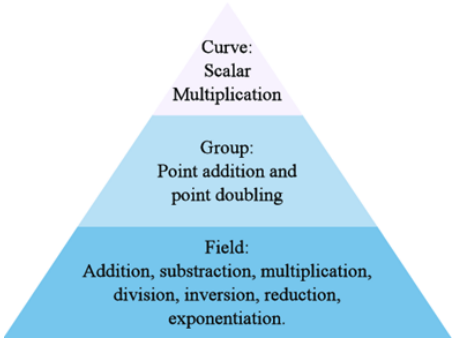

Figure 3: Operations in ECC divided by levels.[21]

Precomputing the points will help faster computation at level 2. Instead of repeating the addition and doubling many times, precomputation will increase the overall performance of the scalar and ECC protocols. This include point Tripling $3P$, point Quintupling $5P$, and point Septupling $7P$ in addition to other precomputed points [22] and [23].

Point Septupling $7P$ is to find $(x_7,\ y_7)$ by calculating the 7-fold of the point $P = (x, y)$. According to [24] who proposed the first Septupling formula of the point introduced by [25], the Septupling is calculated over the affine binary field to be used for multi-base number (MTB) as a scalar recoding. Its cost is $3i+7s+18m$, where $i,\ s,\ and\ m$ is denote the cost of inversion, squaring, and multiplication respectively. Later, [26] proposed a new $7P$ calculation over binary field in terms of affine coordinates, the cost of the proposed

algorithm is $2i + 7s + 14m$. In [27], the authors studied the literature on multiplying an odd scalar to the point P over prime field. They found that Sakai's method which uses the formula [α + $4d$ + 1 + $4d$ + 1 β] to calculate the cost gives the best performance with an overall cost of 67 operations. In [28], the authors proposed a new Septupling point $7P$formula in Jacobian coordinates and used it in the multi-base non-adjacent form (mbNAF) and Window-based (wmbNAF) methods. The cost over Jacobian is $14m$ + $15s$. Similarly in [24], they proposed a new point Septupling $7P$ formula for triple-based chain (TBC) representation of the scalar using {2, 3, 7}-basis over prime field. Similarly, they used Co_Z operation method and calculate the overall cost of the triple-based together.

2. Motivation

According to NIST report [29] page 88, using binary field in ECC is outperforms the prime field since it yields the same level of security with smaller key size (163 vs. 192). In addition, using Lopez-Dahan LD coordinate over the binary curve yields the best performance for ECC [30], [22], [23] and [31]. Over the binary curves, most known formulas for adding points together are incomplete [32]. Also, in literature, the precomputed formula of the point Septupling $7P$ is not available [31] and [33]. Thus, the point Septupling can be efficiently implemented by scalar multiplication such as $w-NAF$, double or multi-base numbering system. In view of the aforementioned, the contributions of this are as follows:

- A new precomputed Septupling point $7P$ arithmetic formula is proposed for LD coordinate over the binary curve using the form $7P = 6P + P$ using mixed addition.
- A new precomputed Sixtupling point $6P$ arithmetic formula is proposed for LD coordinate over the binary curve using the form $6P = 3(2P)$ using mixed addition which is to be deployed in the Septupling precomputed formula.

The remaining sections of this paper are organized as follows: Section 2 introduces the literature and related work. Section 3 presents the proposed formulas, and finally Section 4 concludes the paper and highlights suggestions for future work.

3. Literature Review

Elliptic curve cryptography ECC utilizes the elliptic curve over a finite field F_q, denoted by $E(\mathbb{F}_q)$ which contains the points $(x, y) \in \mathbb{F}_q \; x \; \mathbb{F}_q$ that is in affine coordinates and satisfy Weierstrass as provided in Equation (1).

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \tag{1}$$

Where $a_i \in \mathbb{F}_q$

The point at infinity $\mathcal{O}$ is a special point that form abelian group with the finite field $E(\mathbb{F}_q)$, where $\mathcal{O}$ is a neutral element in the group operation [7].

Over ECC, different forms for a_i will represent different curves. Some curves are suitable for use in the prime field such as short Weierstrass curve which uses the form in Equation (2), Barreto-Naehrig curve which uses the form in Equation (3) below, as well as other curves. Although there are several applicable formulas within the family of binary curves, the most suitable curve for the binary field is Koblitz curve as shown in Equation (4), where $a \in \{0,\ 1\}$.

$$y^2 = x^3 + ax + b \tag{2}$$

$$y^2 = x^3 + b \tag{3}$$

$$y^2 + xy = x^3 + ax^2 + 1 \tag{4}$$

Anomalous binary curve (ABC) or Koblitz curve is recommended by NIST standard [29] for the curve $K-163$ *where* $a = 1$. It allows for fast and efficient scalar multiplication while efficiently using both hardware and software. Particularly, it is attractive because of its lightweight implementation [34]. Over LD projective coordinates, the equation of the projective point $(X : Y : Z)$ where $Z \neq 0$ has its Equation as shown in (5) [35] .

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \tag{5}$$

The first proposed point addition over LD by [36] costs $6S + 14M + 8A$ as provided in the formula in Equation (6) below.

$$(X_0, Y_0, Z_0) + (X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$$
$$Where:$$
$$A_0 = Y_1.Z_0$$
$$A_1 = Y_0.Z_1^2$$
$$B_0 = X_1.Z_0$$
$$B_1 = X_0.Z_1$$
$$C = A_0 + A_1$$
$$D = B_0 + B_1$$
$$E = Z_0.Z_1$$
$$F = D.E$$
$$Z_2 = F^2$$
$$G = D^2.(F + aE^2)$$
$$H = C.F$$

$$X_2 = C^2 + H + G$$
$$I = D^2.A_0 + X_2$$
$$J = D^2.A_0 + X_2$$
$$Y_2 = H.I + Z_2.J \tag{6}$$

To reduce the cost, the formula in (6) can be improved when $Z = 1$ for its special case as shown in the formula provided in Equation (7).

$$(X_0, Y_0, Z_0) + (X_1, Y_1, 1) = (X_2, Y_2, Z_2)$$
$$Such\ that:$$
$$A = Y_1.Z_0^2 + Y_0$$
$$B = X_1.Z_0 + X_0$$
$$C = Z_0.B$$
$$D = B_2.(C + aZ_2)$$
$$Z_2 = C^2$$
$$E = A.C$$
$$X_2 = A^2 + D + E$$
$$F = X_2 + X_1.Z_2$$
$$G = X_2 + Y_1.Z_2$$
$$Y_2 = E.F + Z_2.G \tag{7}$$

The cost was reduced later by [37] who introduced a new formula with cost $4S + 13M + 9A$. Afterwards, [38] proposed a new formula which reduces the cost of the point addition using mix addition techniques in the projective as shown in the formula provided in Equation (8) below.

$$(X_1, Y_1, 1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$$
$$Where:$$
$$U = Z_2^2\ Y_1$$
$$S = Z_2\ X_1 + X_2$$
$$T = Z_2\ S$$
$$Z_3 = T^2$$
$$V = Z_3\ X_1$$
$$X_3 = U^2 + T(U + S^2 + a_2T)$$

$$Y_3(V + X_3)(TU + Z_3) + Z_3^2(Y_1 + X_1) \tag{8}$$

The point doubling $2P$ implies adding the point P to itself such that $2P = P + P$. The first proposed $2P$ over LD coordinate as the projected form is as shown in the following Formula provided in Equation (9) below with the cost $4S + 5M + 5A$ [36].

$$\begin{gathered}
2(X_1.Y_1, Z_1) = (X_3, Y_3, Z_3) \\
Where \\
A = Z_1^2 \\
B = bA^2 \\
C = X_1^2 \\
Z_3 = AC \\
X_3 = C^2 + B \\
Y_3 = (Y_1^2 + aZ_3 + B)\ X_3 + Z_3\ B
\end{gathered} \tag{9}$$

Later, [39] improved the cost of the point doubling to $4S + 5M + 5A$. The proposed projective form is as shown in in the formula provided in Equation (10) below:

$$\begin{gathered}
2(X_1, Y_1, Z_1) = (X_3, Y_3, Z_3) \\
Where \\
S = X_1^2 \\
U = S + Y_1 \\
T = X_1 Z_1 \\
Z_3 = T^2 \\
T = UT \\
X_3 = U^2 + T + a_2 Z_3 \\
Y_3 = (Z_3 + T)\ X_3 + S^2 Z_3
\end{gathered} \tag{10}$$

Using these formulas, different point compositions have been implemented such as point Tripling $3P$ using the mixed addition, and using the projective form for LD coordinate over binary coordinates. The best cost point Tripling uses the form $3P = 2P + P$ proposed by [22], with a cost of $7S + 12M$ where the addition were neglected. A new two Quintupling points $5P$ was also proposed by [23] using two forms; $5P = 3P + 2P$ and the form $5P = 2(2P) + P$ with cost of $13S + 23M$ and $12S + 17M$ respectively outperforming the former with respect to the second form.

4. Proposed Algorithm

This paper introduces a new formula for point Septupling $7P$ for the projective coordinates using affine LD over short Weiestrass curve. To achieve a higher performance, the mixed formula is used for addition in the affine. The proposed point Septupling used the form $7P = 2(3P) + P$.with details shown in Algorithm 1.

Algorithm 1: A new Septupling point of the form $7P = 2(3P) + P$ using LD coordinate in affine and mixed addition over binary curve.

Let the point $P = (X_1,\ Y_1,\ Z_1)$ be a point on the Weiestrass curve as $Y^2 + X\ Y = X^3 + aX^2 + b$ using LD coordinate, let the points $2P$, $3P$, and $6P$ is $(X_2,\ Y_2,\ Z_2)$, $(X_3,\ Y_3,\ Z_3)$ and $(X_6,\ Y_6,\ Z_6)$ respectively. Then the $7P$ formula is formulated as shown below:

First, the Doubling point $2P$ is found using the Formula in (10) as shown in (11) below:

$$
\begin{gathered}
2(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2) \\
A_2 \leftarrow X_1^2 \\
B_2 \leftarrow A_2 + Y_1 \\
C_2 \leftarrow X_1\ Z_1 \\
D_2 \leftarrow B_2\ C_2 \\
Z_2 \leftarrow C_2^2 \\
X_2 \leftarrow B^2 + D_2 + a\ Z_2 \\
Y_2 \leftarrow (Z_2 + D_2)\ X_2 + A_2^2\ Z_2 \\
Cost\ of\ Doubling\ point\ is : 4S + 5M
\end{gathered} \tag{11}
$$

Then, finding the Tripling point $3P$ using (8) yields the formula in (12) below:

$$
\begin{gathered}
(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)\ such\ that\ Z_1 = 1 \\
A_3 \leftarrow Y_2 + Y_1\ Z_2^2 \\
B_3 \leftarrow X_2 + X_1\ Z_2 \\
C_3 \leftarrow B_3\ Z_2 \\
Z_3 \leftarrow C_3^2 \\
D_3 \leftarrow X_1\ Z_3 \\
X_3 \leftarrow A_3^2 + C_3(A_3 + B_3^2 + a\ C_3) \\
Y_3 \leftarrow (D_3 + X_3)(A_3\ C_3 + Z_3) + (Y_1 + X_1)\ Z_3^2 \\
Cost\ of\ Doubling\ point\ is : 5S + 9M
\end{gathered} \tag{12}
$$

Both the formulas in (11) and (12) can be used to find the Sixtupling point $6P$ as shown in (13) below:

$$\begin{gathered}
6P = 2(3P) = (X_6, Y_6, Z_6) = 2 * (X_3, Y_3, Z_3) \\
A_6 \leftarrow X_3^2 \\
B_6 \leftarrow A_6 + Y_3 \\
C_6 \leftarrow X_3 \ Z_3 \\
D_6 \leftarrow B_6 \ C_6 \\
Z_6 \leftarrow C_6^2 \\
X_6 \leftarrow B_6^2 + D_6 + a \ Z_6 \\
Y_6 \leftarrow (Z_6 + D_6) \ X_6 + A_6^2 \ Z_6 \\
Cost \ of \ Doubling \ point \ is : 4S + 5M
\end{gathered} \tag{13}$$

Finally, the Septupling point $7P$ is found using the form $7P = 6P + P$ using the formulas in (10) and (13) as shown in (14) below:

$$\begin{gathered}
(X_7, Y_7, Z_7) = (X_1, Y_1, Z_1) + (X_6, Y_6, Z_6) \ such \ that \ Z_1 = 1 \\
A_7 \leftarrow Y_6 + Y_1 \ Z_6^2 \\
B_7 \leftarrow X_6 + X_1 \ Z_6 \\
C_7 \leftarrow B_7 \ Z_6 \\
Z_7 \leftarrow C_7^2 \\
D_7 \leftarrow X_1 \ Z_7 \\
X_7 \leftarrow A_7^2 + C_7(A_7 + B_7^2 + C_7 \ a) \\
Y_7 \leftarrow (D_7 + X_7)(A_7 \ C_7 + Z_7) + (Y_1 + X_1) \ Z_7^2 \\
Cost \ of \ Doubling \ point \ is : 5S + 9M
\end{gathered} \tag{14}$$

The cost of the point is obtained by adding the number of squaring to number of multiplications. So, the Septupling point cost is the total of cost of Formulas (11), (12), (13), and (14); which 19 $S + 28$ M, while the Sixtupling point's cost is the total cost of (11), (12) and (13); which 14 $S + 19$ M.

To prove the Septupling point, a non-supersingular affine coordinate is used over the binary field $E(\mathbb{F}_{2^m})$ for the equation $y^2 + xy = x^3 + ax^2 + b$ which includes the set of points $P(x, y)$ such that $x, y \in \mathbb{F}_{2^m}$. Proof of the used method follows from [38], [22], [40], [23] and [31] and proposed as in Lemma (1) below.

Lemma 1: The proposed Septupling point of form $7P = 2(3P) + P$ has a valid formula.

Proof:

To prove the formulas in Algorithm 1, the Affine coordinate is used. In Affine coordinates, for adding the two points $(X_7, Y_7, Z_7) = (X_1,\ Y_1,\ Z_1) + (X_6, Y_6, Z_6)$ the following equations should be satisfied:

$$\begin{aligned} \lambda &= \frac{(y_6 + y_1)}{(x_6 + x_1)} \\ x_7 &= \lambda^2 + \lambda + x_6 + x_1 + a \\ y_7 &= \lambda(x_1 + x_7) + x_7 + y_1 \end{aligned} \tag{15}$$

Using Formulas (11), (12), (13), and (14), the forms $\frac{X_7}{Z_7} = x_7$ and $\frac{Y_7}{Z_7^2} = y_7$ needs to be proven. The process is:

$$\begin{aligned} \frac{X_7}{Z_7} &= \frac{A_7^2 + C_7(A_7 + B_7^2 + aC_7)}{C_7^2} = \frac{A_7^2}{C_7^2} + \frac{A_7}{C_7} + \frac{B_7^2}{C_7} + a \\ &= \frac{(Y_6 + Y_1 Z_6^2)^2}{(B_7 Z_6)^2} + \frac{Y_6 + Y_1 Z_6^2}{B_7 Z_6} + a \\ &= \frac{(Y_6 + Y_1 Z_6^2)^2}{(X_6 + X_1 Z_6)^2 (Z_6)^2} + \frac{Y_6 + Y_1 Z_6^2}{(X_6 + X_1 Z_6) Z_6} + \frac{X_6 + X_1 Z_6}{Z_6} + a \\ &\quad Let\ Z_6 = 1 \\ &= \frac{(Y_6 + Y_1)^2}{(X_6 + X_1)^2} + \frac{Y_6 + Y_1}{X_6 + X_1} + X_6 + X_1 + a \\ &= (\frac{Y_6 + Y_1}{X_6 + X_1})^2 + \frac{Y_6 + Y_1}{X_6 + X_1} + X_6 + X_1 + a \\ &= (\frac{Y_6 + Y_1/Z_1^2}{X_6 + X_1/Z_1})^2 + \frac{Y_6 + Y_1/Z_1^2}{X_6 + X_1/Z_1} + X_6 + \frac{X_1}{Z_1} + a \\ &= (\frac{y_6 + y_1}{x_6 + x_1})^2 + \frac{y_6 + y_1}{x_6 + x_1} + x_6 + x_1 + a \\ x_7 &= \lambda^2 + \lambda + x_6 + x_1 + a \ \ (As\ x_7\ form\ in\ Formula\ (15)) \end{aligned} \tag{16}$$

$$\begin{aligned} \frac{Y_7}{Z_7^2} &= \frac{(D_7 + X_7)(A_7 C_7 + Z_7) + (Y_1 + X_1) Z_7^2}{C_7^4} \\ &= \frac{A_7 C_7 (X_1 Z_7 + D_7) + (Y_1 + X_1) Z_7^2}{C_7^4} \\ &= \frac{(Y_6 + Y_1 Z_6^2)(X_1 Z_7 + X_7)}{C_7^3} + \frac{X_7}{C_7^2} + Y_1 \\ &= \frac{(Y_1 + Y_6/Z_6^2)}{(X_1 + X_6/Z_6)}\ (X_1 + X_7 Z_7) + \frac{X_7}{Z_7} + Y_1 \\ &= \frac{(y_1 + y_6)}{(x_1 + x_6)}\ (x_1 + x_7) + x_7 + y_1 \\ y_5 &= \lambda(x_1 + x_7) + x_7 + y_1 \ \ (Proven\ as\ in\ Formula\ (15)) \end{aligned}$$

5. Conclusion and Future Work

This paper introduces the formula of the Septupling point $7P$, using LD coordinates and a non-Supersingular Affine over the binary field $E(\mathbb{F}_{2^m})$ for the equation $y^2 + xy = x^3 + ax^2 + b$ which includes the set of points $P(x, y)$ such that $x, y \in \mathbb{F}_{2^m}$. The point is using the form $7P = 2(3P) + P$ where the point P is in the Affine and the Sixtupling point $2(3P) = 6P$ form is in the projective coordinates. The cost of the Septupling point is $19\ S + 28\ M$, while the cost of Sixtupling point $6P$ is $14\ S + 19\ M$. The point is not comparable to any Septupling point since it is the first formula for $7P$ over LD coordinate and Affine. Since it is precomputed and precalculated, the point can be used with scalar multiplication operation in ECC operation methods such as $w - NAF$ where $w = 4$ or multi-base scalar multiplication such as {2 3, 7}-base methods. This work can also be improved using other forms if available, and higher point calculations can be precomputed such as Nineupling $9P$ or much higher degrees.

References

[1] N. A. Karim and A. H. Ali. E-learning virtual meeting applications: A comparative study from a cybersecurity perspective. *Indones. J. Electr. Eng. Comput. Sci.*, 24(2):1121–1129, 2021.

[2] M. Hijjawi et al. A novel hybrid prairie dog algorithm and harris hawks algorithm for resource allocation of wireless networks. *IEEE Access*, 11(November):145146–145166, 2023.

[3] N. A. Salameh, A. Elias, and N. F. Karim. Proposed model for measuring acceptance of online ads. *J. Eng. Appl. Sci.*, 100(10):2181–2185, 2016.

[4] S. D. Patil, A. B. Kathole, S. Kumbhare, K. Vhatkar, and V. V. Kimbahune. A blockchain-based approach to ensuring the security of electronic data. *Int. J. Intell. Syst. Appl. Eng.*, 12(11):649–655, 2024.

[5] K. K. Kommineni and A. Prasad. A review on privacy and security improvement mechanisms in manets. *Int. J. Intell. Syst. Appl. Eng.*, 12(2):90–99, 2024.

[6] W. K. Abdulraheem. Performance comparison of xen and hyper-v in cloud computing while using cryptosystems. *Int. J. Adv. Soft Comput. its Appl.*, 14(3):17–30, 2022.

[7] O. M. C. Osazuwa. Confidentiality, integrity, and availability in network systems: A review of related literature. *Int. J. Innov. Sci. Res. Technol.*, 8(12):1946–1955, 2024.

[8] N. A. Karim et al. Performance comparison of hyper-v and kvm for cryptographic tasks in cloud computing. *Comput. Mater. Contin.*, 78(2):2023–2045, 2024.

[9] N. A. Karim et al. Using interface preferences as evidence of user identity: A feasibility study. *Int. J. Data Netw. Sci.*, 8(1):537–548, 2024.

[10] M. I. Adawy, M. Tahboush, O. Aloqaily, and W. Abdulraheem. Man-in-the middle attack detection scheme on data aggregation in wireless sensor networks. *Int. J. Adv. Soft Comput. its Appl.*, 15(2):179–193, 2023.

[11] T. Koroglu and R. Samet. Can there be a two way hash function? *IEEE Access*, 12(January):18358–18386, 2024.

[12] E. Barker, Q. Dang, F. Sheila, K. Scarfone, and P. Wouters. Guide to ipsec vpns. 2020.
[13] M. Al-Shalabi, J. Ababneh, and W. Abdulraheem. A novel adjacent sensors-based mechanism to increase performance of wireless sensor networks. *Int. J. Antennas Propag.*, 2021:1–9, 2021.
[14] O. A. Khashan, N. M. Khafajah, W. Alomoush, and M. Alshinwan. Innovative energy-efficient proxy re-encryption for secure data exchange in wireless sensor networks. *IEEE Access*, 12(February):23290–23304, 2024.
[15] N. A. Karim, H. Kanaker, W. K. Abdulraheem, M. A. Ghaith, E. Alhroob, and A. M. F. Alali. Choosing the right mfa method for online systems: A comparative analysis. *Int. J. Data Netw. Sci.*, 8(1):201–212, 2024.
[16] R. Nadaf, N. B. Sumangala, M. Mandi, and A. Konnur. Symmetric and asymmetric cryptographic approach based security protocol for key exchange. pages 1–6, 2023.
[17] W. K. A. Abdulrahem, H. H. O. Nasereddin, and S. M. H. Fares. Business continuity based on rfid. *Am. Acad. Sch. Res. J.*, 5(3):223–228, 2013.
[18] A. H. Alwan. Novel design of radg automata in crns. 2016.
[19] S. Smadi, O. Almomani, A. Mohammad, M. Alauthman, and A. Saaidah. Vpn encrypted traffic classification using xgboost. *Int. J. Emerg. Trends Eng. Res.*, 9(7):960–966, 2021.
[20] N. A. Karim, O. A. Khashan, H. Kanaker, W. K. Abdulraheem, M. Alshinwan, and A. Albanna. Online banking user authentication methods: A systematic literature review. *IEEE Access*, 12(November):741–757, 2023.
[21] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval. Elliptic curve lightweight cryptography: A survey. *IEEE Access*, 6(November):72514–72550, 2018.
[22] S. Yasin and Z. Muda. Tripling formulae of elliptic curve over binary field in lopez-dahab model. *J. Theor. Appl. Inf. Technol.*, 75(2):212–216, 2015.
[23] W. K. AbdulRaheem, S. B. M. Yasin, N. I. B. Udzir, and M. R. B. K. Ariffin. New quintupling point arithmetic 5p formulas for lŏpez-dahab coordinate over binary elliptic curve cryptography. *Int. J. Adv. Comput. Sci. Appl.*, 10(7):397–401, 2019.
[24] S. Liu and L. Zhang. Efficient septuple formula for elliptic curve and efficient scalar multiplication using a triple-base chain representation. *IEEE Access*, 9(4):129512–129520, 2021.
[25] G. N. Purohit and A. Singh Rawat. Fast scalar multiplication in ecc using the multi base number system. *IJCSI Int. J. Comput. Sci. Issues*, 8(1):1–11, 2011.
[26] Z. Lai, Z. Zhang, and D. Tao. Algorithm for directly computing 7p elliptic curves and its application. *J. Comput. Appl.*, 33(7):1870–1874, 2013.
[27] M. Rasmi, H. Mimi, and M. S. Daoud. Evaluating composite ec operations and their applicability to the on-the-fly and non-window multiplication methods. *Int. J. Comput. Appl.*, 105(6):19–26, 2014.
[28] P. Longa and C. Gebotys. Fast multibase methods and other several optimizations for elliptic curve scalar multiplication. 5443:443–462, 2019.
[29] NIST. Digital signature standard (dss). 2013.
[30] B. Rashidi. A survey on hardware implementations of elliptic curve cryptosystems.

arXiv Prepr. arXiv1710.08336, 2017.

[31] Z. Razali, N. Muslim, S. Kahar, and F. Yunos. Implementation of quintupling formula in q-naf. *NeuroQuantology*, 20(8):1339–1344, 2022.

[32] T. Pornin. Efficient and complete formulas for binary curves. *Cryptol. ePrint Arch.*, 9(4):1–29, 2022.

[33] Z. Razali, N. Muslim, S. Kahar, F. Yunos, and K. Mohamed. Improved point 5p formula for twisted edwards curve in projective coordinate over prime field. pages 498–502, 2022.

[34] S. Chowdhury, D. B. Roy, and D. Mukhopadhyay. A minimalistic perspective on koblitz curve scalar multiplication for fpga platforms. 2020-Octob:70–75, 2020.

[35] P. K. Vishnubhai. Design and implementation of efficient elliptic curve cryptography on reconfigurable platforms. 2023.

[36] R. López and J. Dahab. Improved algorithms for elliptic curve arithmetic in gf(2n). 97(107):201–212, 1999.

[37] A. Higuchi and N. Takagi. Fast addition algorithm for elliptic curve arithmetic in gf(2n) using projective coordinates. *Inf. Process. Lett.*, 76(3):101–103, 2000.

[38] E. Al-Daoud, R. Mahmod, M. Rushdan, and A. Kilicman. A new addition formula for elliptic curves over gf(2n). *IEEE Trans. Comput.*, 51(8):972–975, 2002.

[39] T. Lange. A note on lópez-dahab coordinates. *Tatra Mt. Math. Publ.*, 24(33):1–7, 2006.

[40] M. M. Ahmad, S. M. Yasin, R. Mahmod, and M. A. Mohamed. X-tract recoding algorithm for minimal hamming weight digit set conversion. *J. Theor. Appl. Inf. Technol.*, 75(1):109–114, 2015.