*Asian Journal of Research in Computer Science*

*14(4): 228-237, 2022; Article no.AJRCOS.94995*
*ISSN: 2581-8260*

# Efficient Elliptic Curve Arithmetic for Lightweight Cryptographic Schemes for IoT Applications

**Zakaria Abukari [a*], Edward Yellakuor Baagyere [b] and Mohammed Muniru Iddrisu [c]**

*[a] Department of Computer Science, Tamale Technical University, Tamale, Ghana.*
*[b] Department of Computer Science, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.*
*[c] Department of Mathematics, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.*

***Authors' contributions***

*This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.*

***Article Information***

DOI: 10.9734/AJRCOS/2022/v14i4307

**Open Peer Review History:**
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/94995

***Original Research Article***

***Received 12 October 2022***
***Accepted 20 December 2022***
***Published 23 December 2022***

## ABSTRACT

The Internet of Things' (IoT) market is expected to grow exponentially at the global level in the coming years, due to the proliferation of more reliable and faster networks resulting from the extensive rollout of 5 to 10 G mobile networks. By 2025, it is expected that worldwide projection of IoT connected devices will be pegged at 30.9 billion units. Despite the potential benefits of the new technology, security in IoT is a major threat. According to HP, 70% of IoT devices are vulnerable to sniffing attacks and reliable solution is yet to be found. The standard cryptographic algorithms such as RSA and AES provide good security but their utilization in IoT is questionably due to hardware and energy constraints for computationally expensive encryption schemes. However, elliptic curve-based cryptography, a recent paradigm in public key cryptography, achieves the same level of security with smaller key sizes. On the other hand, the total score of performance of an elliptic curve-based cryptosystem depends largely on the efficiency of the arithmetic operations performed in it. It is against this background that this paper proposes efficient elliptic curve arithmetic for implementing ECC based schemes suitable for IoT systems implementations. Elliptic curve point arithmetic implementations in projective coordinate systems over binary extension fields introduce higher efficiencies in software. In this regard, this paper has proposed an improved López-Dahab

**Corresponding author: E-mail: zack@tatu.edu.gh;*

point arithmetic methods on non-supersingular elliptic curves over $GF(2^m)$. The results show 69.20% improvement in Point Doubling, 44.68% in Point Addition and the scalar point multiplication execution time is decreased by 48.80%.

*Keywords: ECC; security; galois fields; field arithmetic; point arithmetic; ECSM; projective coordinate.*

## 1. INTRODUCTION

The Internet of Things (IoT) is considered the most recent upgrade of the existing Internet and various Information and Communication Technology (ICT) tools. It envisions a very near future of total connectivity, interaction and ubiquity among objects of everyday life, industrial equipment, vehicles and practically all physical devices hence the term 'Things' [1].

Currently, security is a major threat to the IoT vision. IoT security borders on protecting stored data and data in transit against eavesdropping, redirection or illegal altering during devices' communications. According to HP, 70% of IoT devices are vulnerable to sniffing attacks and reliable solution is yet to be found [2].

Elliptic curve-based cryptographic schemes were first proposed as the foundation for security framework in Internet of Things and Cloud Computing [3]. In another study on lightweight cryptographic algorithms suitable for data security and authentication in IoT, [4] noted that the standard cryptographic algorithms such as RSA and AES provide good security but their utilization in IoT is questionably due to hardware and energy constraints for computationally expensive encryption schemes whilst ECC achieves the same level of security with smaller key sizes (Table 1).

On the other hand, the total score of performance of an elliptic curve based cryptosystem depends largely on the efficiency of the arithmetic operations performed in it [5]. It is against this background that this paper proposes efficient elliptic curves arithmetic for implementing elliptic curve based schemes.

## 2. ARITHMETIC OPERATIONS IN ELLIPTIC CURVE CRYPTOGRAPHY

The building blocks of any public key cryptoscheme are its arithmetic operations. ECC arithmetics are put into three groups which include Scalar arithmetic, Point arithmetic and Field arithmetic. Point arithmetic operations include Point Addition and Point Doubling whilst addition, subtraction, multiplication, squaring and inversion in the underlying field constitute the field arithmetic operations [6,7].

The two major fields used in cryptography are prime fields $\mathbb{F}_p$ and binary extension fields, denoted $\mathbb{F}_{p^m}$ or $GF(2^m)$ for some integer $m > 1$. The latter introduce higher efficiencies as compared to the other fields in software implementation [8]. In this regard, efficient methods for the arithmetic involved in implementing elliptic curves over binary extension fields $GF(2^m)$ whereby the order of the curves can be up to $m$ $bit$s is of great importance.

### 2.1 Representation of Elements in $GF(2^m)$

Elements of $GF(2^m)$ are represented in many basis. However the major ones used in cryptography are the Normal Basis (NB), Polynomial Basis (PB) and Redundant Basis (RB), according to [9]. A very remarkable observation is that the choice of the basis by which field elements are represented has a major effect on the implementation of the finite field operations [10,11]. For example, in software implementations of cryptographic schemes, the use of Polynomial Basis yields better results than the Normal Basis [12]. However, when it comes to hardware implementations, for some $GF(2^m)$ operations, using the Normal Basis is more suitable [13].

In the Polynomial Basis, the elements of $GF(2^m)$ are binary polynomials and at most $m-1$ degree. Now let a basis element $\beta \in GF(2^m)$ be a root of an m-degree irreducible polynomial $P(x)$, the set of powers of the basis element $\beta = \{\beta^0, \beta^1, \cdots, \beta^{m-2}, \beta^{m-1}\}$ define a Polynomial Basis for $GF(2^m)$ [9]. Any field element $A \in GF(2^m)$ can therefore be uniquely expressed as

$$A = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{m-1}\beta^{m-1}$$

$$= \sum_{i=0}^{m-1} a_i \beta^i, a_i \in GF(2) \quad (1)$$

**Table 1. Comparison between RSA and ECC**

| Algorithm | Key Size (bits) | Key generation (s) | Signature generation (s) | Signature verification (s) | Merits |
|---|---|---|---|---|---|
| RSA | 1024 | 0.16 | 0.01 | 0.01 | Increased security |
| | 15360 | 679.06 | 9.20 | 0.03 | |
| ECC | 163 | 0.08 | 0.15 | 0.23 | Increased speed, less memory requirement, optimum security |
| | 571 | 1.44 | 3.07 | 4.53 | |

## 2.2 Addition (Subtraction) of $GF(2^m)$ Elements in Polynomial Basis

$$Let\ X = \sum_{i=0}^{m-1} x_i \beta^i, x_i \in GF(2)\ and\ Y = \sum_{i=0}^{m-1} y_i \beta^i, y_i \in GF(2) \quad (2)$$

The additions is given as

$$X + Y = \sum_{i=0}^{m-1} ((x_i + y_i) \bmod 2)\beta^i \quad (3)$$

A careful observation is that Equation (3) is reduced to simply XORing $X\ and\ Y$.

## 2.3 Multiplication of $GF(2^m)$ Elements in Polynomial Basis

Let a $, b \in GF(2^n)$ be represented as polynomials

$$a(x) = \sum_{i=0}^{n-1} a_i x^i \text{ and } b(x) = \sum_{i=0}^{n-1} b_i x^i \quad (4)$$

where $a_i$, $b_i$ $\in$GF(2) or equivalently represented as binary vectors and let

$$p(x) = x^n + r(x)$$

be an irreducible polynomial of degree n over GF(2) the extension field multiplication of $a(x).b(x)$ is given as

$$c(x) = a(x).b(x) = \left(\sum_{i=0}^{n-1} a_i x^i\right).\left(\sum_{j=0}^{n-1} b_j x^j\right) \equiv \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\left(a_i.b_j \bmod p(x)\right).\ x^{(i+j)} = \sum_{k=0}^{2n-2} c_k x^k \quad (5)$$

There are a number of ways of implementing Equation (5). A few of the most recommended approaches are presented here.

The standard Shift-and-Add method [14] computes $a(x)b(x)(mod\ (p(x))$. This is based on the fact that

$$a(x)b(x) = a_{n-1}x^{n-1}b(x) + \cdots + a_1 x b(x) + a_0 b(x) \quad (6)$$

and in that regard, the method computes

$$x^i b(x) \bmod p(x)\ \forall\ 1 \le i \le n-1 \quad (7)$$

and add all the results for which $a_i$ = 1.

The Comba's Right to left and the Left to Right methods (Algorithm 1 and Algorithm 2) that can be interleaved with a polynomial reduction algorithm (Algorithm 3) are some improved versions of the Standard Shift and Add.

In [15], the polynomial representation was used to develop another method of multiplying two elements in GF($2^m$). It was a variant of the original Montgomery's method for modular multiplication of integers.

## 2.4 Field Arithmetic Inversion

Inversions are the most expensive operations among the field arithmetics useful to point arithmetics in elliptic curves cryptography. The multiplicative inverse of an element $a \in GF(2^m)$ is that element $a^{-1}$such that

$$a.a^{-1} = 1 \quad (8)$$

A number of algorithms for both $\mathbb{F}_p$ and $GF(2^m)$ identified in the literature are based on the Euclidean algorithm and the Fermat's Little Theorem (FLT). A premier algorithm using Normal Basis found in [8] remains the generic. It was extended to Polynomial Basis by [16].

## 2.5 Point Arithmetic on Elliptic Curves

Elliptic curves over binary extension fields are two types: Supersingular and Non-supersingular as defined in Equation (9) and Equation (10) respectively. However, for cryptographic applications, recommendations for the use of only non-supersingular curves have come up strongly [17,18].

**Algorithm 1. Right-left comba's method for polynomial multiplication**

**Input:** Binary polynomials a(x) and b(x) of degree at most $m-1$
**Output:** c(x) = a(x).b(x)$of at\ most\ 2m-2\ degree$

1. $C \leftarrow 0$
2 $for\ k = 0\ to\ w-1\ do$
2.1 for j = 0 to t − 1 do
if the $k^{th} bit\ of\ A[j] = 1\ then$
$C\{j\} \leftarrow C\{j\} + B$
2.2 if k ≠ w − 1 then
B ← B.x
3. $Return\ (C)$

**Algorithm 2. Left-to-right comba's method for polynomial multiplication**

**Input:** Binary polynomials a(x) and b(x) of degree at most $m-1$
**Output:** c(x) = a(x).b(x)$of at\ most\ 2m-2\ degree$

1. $C \leftarrow 0$
2 $for\ k = w-1\ \ downto\ 0\ do$
2.1 for j = 0 to t − 1 do
if the $k^{th} bit\ of\ A[j] = 1\ then$
$C\{j\} \leftarrow C\{j\} + B$
2.2 if k ≠ 0 then
C ← C.x
3. $Return\ (C)$

**Algorithm 3. Bit by bit polynomial modular reduction**

**Input:** Binary polynomial c(x) of degree at most $2m-2$, p(x)
**Output:** c(x) (mod p(x))
1. $Precompute\ u_k(x) = x^k r(x)\ for\ all\ x^m r(x), 0 \le k \le w-1$
2. $for\ i = 2m-2\ \ downto\ m\ do$
2.1 $if\ c_i = 1\ then$
$j = \frac{i-m}{w}$
$k = (i-m) - wj$
$C\{j\} \leftarrow u_k(x)$

3. $Return\ \big((C[t-1], \ldots C[1], C[0])\big)$

Let q = $GF(2^m)$,

A supersingular elliptic curve over q is

$$E(q): y^2 + xy = x^3 + ax + b \quad (9)$$

where $a, b \in q$ and $\Delta = -a^3\ is\ the\ discriminant$.

$$E(q): y^2 + xy = x^3 + ax^2 + b \quad (10)$$

where $a, b \in GF(2^m)$ and $b \neq 0\ is\ the\ discriminant$

The set of points on E with coordinates in $GF(2^m)$ is the set

A non-supersingular elliptic curve over q is

$$E(q) = \{(x,y): x, y \in GF(2^m)\ satisfying\ y^2 + xy = x^3 + ax^2 + b \cup \{\mathcal{O}\}\} \quad (11)$$

and

$$\mathrm{E(q) = \{(x,y): x,y \in GF(2\text{^}m)\ satisfying\ [\![ y ]\!]\text{^}(2) + xy = x\text{^}3 + ax + b \cup \{O\}\}} \quad (12)$$

for supersingular and non-supersingular curves respectively.

For a non-supersingular elliptic curve E defined over GF($2^m$) in affine coordinates as in Equation (10), Point Addition and Point Doubling operations are generally computed as follows [17].

**i) Point Addition**

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E, P \neq Q$ and $\mathrm{Q} \neq -\mathrm{P}$, then $\mathrm{P} + \mathrm{Q} = (x_3, y_3)$ where,

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \quad (13)$$
with $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$

**ii) Point Doubling**

Let $P = Q = (x_1, y_1)$ then $P + Q = P + P = 2P = (x_3, y_3)\ where$

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2} \quad (14)$$
$$y_3 = x_1^2 + \lambda x_3 + x_3$$
$$with\ \lambda = x_1 + \frac{y_1}{x_1}$$

A repeated addition is represented as multiplication of a point by an integer. For example, the addition of n times of P as illustrated bellow is considered n multiplied by P.

$$\underbrace{\mathrm{P} + \mathrm{P} + \mathrm{P} + \cdots + \mathrm{P}}_{\text{n copies}} = \mathrm{nP} \quad (15)$$

In this regard, Point Doubling is a special addition instance where P = Q and as such P+Q = P+P, thus reducing the Point Doubling operation to addition of a point to itself. P+P is also denoted as 2P.

### 2.5.1 Projective coordinates

The formulas for both Point Addition and Point Doubling require one field inversion each and field multiplications in either case. The cost of field addition and squaring can be ignored according to the works of [18]. Inversion in GF($2^m$) is very expensive as compared relatively to multiplication. As a result, alternative point representations, called projective cordinates, in which the point arithmetics are performed without inversions are the most prefered. Several types of projective coordinates for the non-supersingular elliptic curves exist. The three most recommended are:

*2.5.1.1 The standard projective coordinates*

In the S*tandard* Projective Coordinates system, the projective point $(X:Y:Z),\ Z \neq 0$ corresponds to the point $(X/Z, Y/Z)$ in the affine system. The corresponding equation of the elliptic curve is presented as

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \quad (16)$$

*2.5.1.2 The jacobian projective coordinates*

The projective point $(X:Y:Z), Z \neq 0$ is mapped to the point $(X/Z^2, Y/Z^3)$ in the affine coordinates. The projective equation is presented as

$$Y^2Z + XYZ = X^3 + aX^2Z^2 + bZ^6 \quad (17)$$

*2.5.1.3 The López-Dahab (LD) projective coordinates*

In this coordinate system, the projective point $(X:Y:Z), Z \neq 0$ corresponds to the affine coordinate point $(X/Z,\ Y/Z^2)$ whilst its projective equation is

$$Y^2Z + XYZ = X^3Z + aX^2Z^2 + bZ^4 \quad (18)$$

Table 2 has a summary of computational cost analyses of the point operations in the three projective coordinate systems and the affine coordinate [12]. The counts of field multiplications (M) and field inversions (I) are measured in each system.

## 2.6 Scalar Arithmetic

The scalar arithmetic, which involves the multiplication of a scalar *k* by a point *P,* denoted $kP$, is considered the most dominant and time consuming operation, estimated to take about

**Table 2. Field arithmetic operations count in point arithmetic on non-supersingular curves**

| Coordinate system | General addition | General addition (mixed) | Doubling |
|---|---|---|---|
| Affine | 1 I + 2M | - | 1 I + 2M |
| Standard projective | 13M | 12M | 7M |
| Jacobian projective | 14M | 10M | 5M |
| López-Dahab projective | 14M | 8M | 4M |

80% of the total execution time of any elliptic curve cryptographic scheme [19]. Over the years, a myriad of proposed techniques to provide efficient implementations of the scalar multiplication have emerged in the literature. A good survey on $kP$ is found in [20].

## 2.7 Summary of Findings from the Literature

The elliptic curve scalar multiplication, being the most expensive operation in the overall elliptic curve based encryption/decryption, relies on the point arithmetic, which in turn, relies on the underlying field arithmetics. Surveys on various ECSM indicate that the field inversion is very expensive as compared relatively to multiplication and squaring, and it is responsible for the high computational overhead in ECSM [20,21,22,23]. The cost of field addition and squaring can be ignored [18]. Bhardwaj, et al. Houssain, et al. [5] did a computational cost analysis of these operations over $\mathrm{GF}(2^m)$ and established that the cost of field addition is negligible; field inversion is equivalent to ten times field multiplication; and field squaring is approximately 0.2 times field multiplication.

In terms of implementation, field addition (subtraction) of two elements $\mathrm{a}, \mathrm{b} \in GF(2^m)$ can be achieved simply by a bitwise XORing of $\mathrm{a}$ and $\mathrm{b}$ whilst multiplication and squaring using Polynomial Basis are quite simple in software implementation.

# 3. PROPOSED EFFICIENT ARITHMETICS FOR IMPLEMENTATION

The summary of findings from the literature suggests that, for efficient implementation of ECC, the scalar point multiplication methods devoid of field inversions will be lighter and yield faster speed encryptions/decryptions, and as such very suitable for real-time IoT applications. In this regard, this paper proposes as follows:

## 3.1 Proposed Point Arithmetic

From the data in Table 2, one can appreciate that Point Addition and Point Doubling methods in the López-Dahab projective coordinate system offer the minimum field multiplications count and they do not require the computational expensive field inversions, and for that matter, the best alternative. However, a critical analyses of the addition and multiplication formulas and algorithms, as they are presented in [24], reveals that, for software implementation, more improvements can be done to further improve performance of the López-Dahab methods as follows:

### 3.1.1 Introduction of concurrency

The algorithms are executed in a step-by-step approach even if a previous step does not have dependencies in the preceding steps. Introducing multi-threading into these methods, otherwise termed concurrent processing, will be apt, in order to allow non-dependent segments to execute at the same time. This is expected to reduce the execution time although the field operations' counts will remain the same. In this regard, concurrent execution is proposed in Algorithm 4 and Algorithm 5.

A caveat to this proposal is that some IoT devices may not have multicore technology. Notwithstanding, the issues on architecture dependencies, massive scaling and design challenges of IoT based Industrial applications, in addition to security, are still in contention [25]. Moreover, multicore processors are becoming mass products and as such it is not farfetched to conceive the notion that the upcoming IoT devices will be multicore compliant.

## 3.2 Proposed Scalar Point Multiplication

From the literature, two main efficient approaches are used: binary methods and Windows based methods. Except a very few but with more computational overheads, majority of the methods are based on the binary expansion of the scalar

$$k = (k_{m-1}, k_{m-2}, \cdots, k_0)$$

and perform either Point Doubling and/or Point Addition depending on the value of $k_i$. In this regard, this paper proposes the interleaving of any efficient method with Algorithms 4 and 5. An example is presented in Algorithm 6.

**Algorithm 4. Multi-thread lópez-dahab point doubling**

Input: $P = (X_1 : Y_1 : Z_1)$ in LD Coordinates on E: $y^2 + xy = x^3 + ax^2 + b$
Output: $2P = (X_3 : Y_3 : Z_3)$ in LD Coordinates
1. if $P = \infty$ then return $(\infty)$
2. Thread1{ $Z_3 \leftarrow X_1^2 Z_1^2$ } // end of thread 1
3. Thread2 {$X_3 \leftarrow X_1^4 + bZ_1^4$ } // end of Thread2

Thread3 Starts
4. if $a = 1$ then $T_1 \leftarrow aX_1^2 Z_1^2 + Y_1^2$
5. $T_1 \leftarrow aX_1^2 Z_1^2 + Y_1^2 + bZ_1^4$
6. $Y_3 \leftarrow (X_1^4 + bZ_1^4).T_1$
7. $Y_3 \leftarrow Y_3 + bZ_1^4.X_1^2 Z_1^2$ }

Thread3 ends
8. Wait for multiple threads

Return $(X_3 : Y_3 : Z_3)$

**Algorithm 5. Multi-thread lópez-dahab point addition**

**Input**: $P_1 = (X_1 : Y_1 : Z_1)$ in LD projective coord, $P_2 = (x_2, y_2)$ in affine coordinate system on $E: y^2 + xy = x^3 + ax^2 + b$
**Output**: $P_1 + P_2 = (X_3 : Y_3 : Z_3)$ in LD coordinates
*1.* if $P_2 = \infty$ then return $(P_1)$
*2.* if $P_1 = \infty$ then return $(x_2 : y_2 : 1)$
*3.* $T_1 \leftarrow Z_1.x_2$
*4.* $T_2 \leftarrow Z_1^2$
*5.* $X_3 \leftarrow X_1 + X_2 Z_1$
*6.* $T_1 \leftarrow Z_1.X_3$
*7.* $T_3 \leftarrow T_2.y_2$
*8.* $Y_3 \leftarrow Y_1 + T_3$
*9.* If $X_3 = 0$ then
9.1 if $Y_3 = 0$ then use Point doubling algorithm for computing
$(X_3 : Y_3 : Z_3) = 2(x_2 : y_2 : 1)$ *and* return $(X_3 : Y_3 : Z_3)$
9.2 else return$(\infty)$

$T_4 \leftarrow T_1^2$

**Thread1 Starts**
*10.* $Z_3 \leftarrow T_4$
*11.* $T_3 \leftarrow T_1.Y_3$
*12. If a =1 then* $T_1 \leftarrow T_1 + T_2$
*13.* $T_2 \leftarrow X_3^2$
*14.* $X_3 \leftarrow T_2.T_1$
*15.* $X_3 \leftarrow X_3 + Y_3^2$
*16.* $X_3 \leftarrow X_3 + T_3$
*17.* $T_2 \leftarrow x_2 T_4 + X_3$
**Thread1 Ends**
**Thread2 Starts**
*18.* $T_1 \leftarrow T_4^2$
*19.* $T_3 \leftarrow T_3 + T_4$
*20.* $T_5 \leftarrow x_2 + y_2$
*21.* $T_6 \leftarrow T_1.T_5$
**Thread2 Ends**
*22. Wait for multiple threads*
*23.* $Y_3 \leftarrow T_3.T_2$
*24.* $Y_3 \leftarrow Y_3 + T_6$
*25.* Return $(X_3 : Y_3 : Z_3)$

## 4. KEY PERFORMANCE ANALYSIS

In order to measure the performance of the proposed Multi-Thread López-Dahab (MTLD) Point Addition and Point Doubling, the original López-Dahab algorithms and the proposed were implemented in Borland Delphi on Intel Core i3 running Windows 10. Comparing the proposed to the original López-Dahab algorithms, a remarkable decrease in the running time was observed as presented in Table 3 and Fig. 1. Point Doubling has seen 69.20% improvement whilst the Point Addition is improved by 44.68%. The scalar point multiplication execution time is decreased by 48.80%. These findings prove that the proposed MTLD is yet a further improvement of the most efficient point and scalar ECC arithmetic, a result that is much desired for IoT real-time applications.

**Table 3. Running time (in μs) comparison between LD and proposed MTLD**

| Operation/ Method | López-dahab | MTLD | Improvement (%) |
|---|---|---|---|
| Point Doubling | 940 | 289 | 69.20 |
| Point Addition | 1860 | 1029 | 44.68 |
| Scalar Point Multiplication | 2930 | 1500 | 48.80 |

**Algorithm 6. Left to right operand scanning method for kp using improved lópez-dahab point arithmetic**

**Input**: Integer $k = (k_{n-1}, k_{n-2}, \cdots k_1, k_0)$, Point $\mathrm{P} \in \mathrm{E}(\mathbb{F}_{2^n})$
**Output**: Point *R* = *kP*.
$R \leftarrow \infty$ // Initialization of R
1. **For** $\mathrm{i} = \mathrm{n} - 1$ **downto** $0$ **do**
   2.1 $R \leftarrow 2R$ // PDBL using Algorithm 4
   2.2 **if** $k_i = 1$ **then** $R \leftarrow R + P$ //PADD using Algorithm 5
3. Return (R)

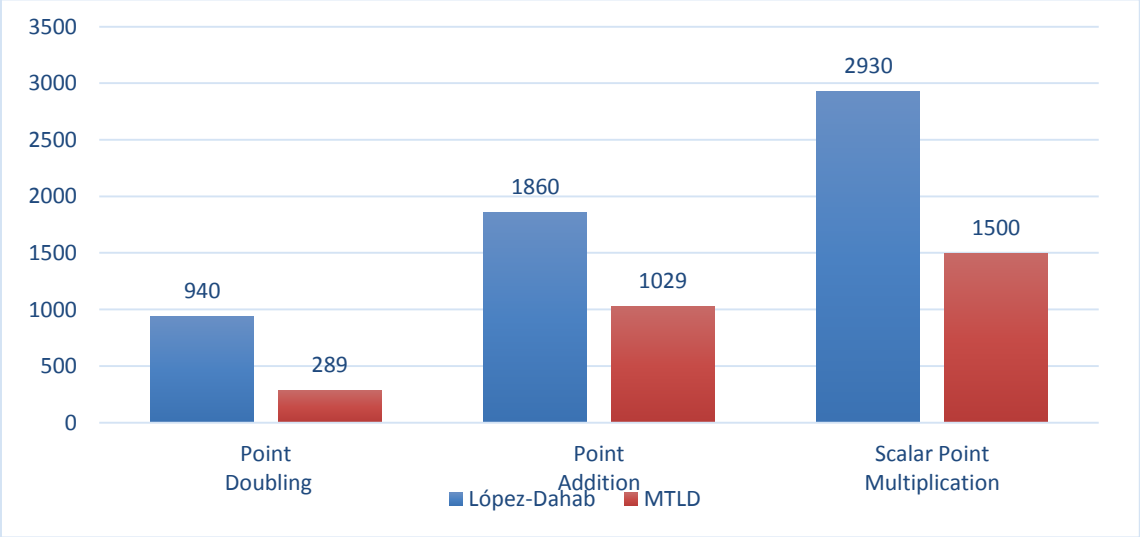


**Fig. 1. Running time (in μs) comparison between LD and proposed MTLD**

## 5. CONTRIBUTION OF THE RESEARCH

The results of this research are especially significant to cryptography. The improved arithmetic can be used in elliptic curve-based cryptoschemes to obtain higher speed encryptions and decryptions. This is very desirous in real-time applications which will soon be dominated by IoT systems.

## 6. CONCLUSION

In this work, proposed efficient elliptic curve arithmetic for implementing ECC based schemes suitable for Internet of Things' applications is presented. The elliptic curve scalar multiplication (ECSM), being the most expensive operation in an elliptic curve based cryptoscheme, relies on the point operations which also depend on the efficiency of the field arithmetic of the underlying finite field. Field inversion in $GF(2^m)$ is very expensive as compared relatively to multiplication and squaring and it is responsible for the high computational overhead in ECSM. Most of the existing methods are implemented over prime fields that cannot avoid field inversions. However, elliptic curve point arithmetic implementations in projective coordinate systems over binary extension fields introduce higher efficiencies in software by avoiding field inversion operations.

A premier method is the López-Dahab point arithmetic methods on non-supersingular elliptic curves over $GF(2^m)$. However, we discovered that further enhancements could be made to that method. In this regard, a proposal is made for incorporating concurrent processing into the López-Dahab projective coordinates point arithmetic methods which are currently non-parallel algorithms.

Addition and subtraction of two elements $\mathrm{a}, \mathrm{b} \in GF(2^m)$ were achieved by simply XORing *a* and *b*. Comba's product scanning algorithms for multiplication of two elements $\mathrm{a}, \mathrm{b} \in GF(2^m)$ were implemented using polynomial basis for their reported performance in the literature.

A prototype implementation of the existing López-Dahab algorithms and our proposed improved methods was done for performance analysis. The execution time was measured for comparison. The results have shown that the proposed methods yield 69.20% and 44.68% improvement in Point Doubling and Point Addition respectively, whilst the scalar point multiplication's execution time is decreased by 48.80%.

## 7. FUTURE WORKS

We intend to use the improved arithmetic to implement the Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE) protocol which shall then be used to develop encryption and decryption schemes suitable for IoT applications.

It is also our desire to further our research in projective coordinates in $GF(2^m)$ in order to develop an improved version of this work that does not use multi-threading approach since some IoT devices may not support multi-core technology.

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES


1. Holdowsky J, Mahto M, Raynor ME, Cotteleer M. Inside the Internet of Things (IoT). [Online]; 2015.
2. Kumar SA, Vealey T, Srivastava H. Security in internet of things: Challenges, solutions and future directions. 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA; 2016.
3. Bai TDP, Rabara AS, Jerald V. "Elliptic curve cryptography based security framework for internet of things and cloud computing. International Journal of Computer Science and Technology [IJCST]. 2015;6:223-229.
4. Bhardwaj I, Kumar A, Bansal M. A review on lightweight cryptography algorithms for data security and authentication in IoTs. 4th IEEE. International Conference on Signal Processing, Computing and Control (ISPCC), Solan; 2017.
5. Houssain H. Elliptic curve cryptography algorithms resistant against power analysis attacks on resource constrained devices, Clermont-Ferrand II: Université Blaise Pascal; 2012.
6. Ranger S. "What is the IoT? Everything you need to know about the internet of things right now," [Online]; 2018. Available:https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
7. Menezes J, van Oorschot PC, Vanstone SA. Handbook of applied cryptography, Florida: CRC Press; 1996.
8. Hosseinzadeh Namin P. Efficient implementation of finite field multipliers over binary extension fields, electronic theses and dissertations. 5828; 2016. Available:https://scholar.uwindsor.ca/etd/5828

9. Lidl R, Niederreiter H. Introduction to finite fields and their applications, NY, USA: Cambridge University Press, second ed; 1997.
10. Gartner Inc., "Gartner says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," [Online]; 2017. Available:https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.
11. Mark P, Shangkuan J, Thomas C. "What's new with the Internet of Things?," [Online]; 2017. Available:https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things
12. Hankerson D, Hernandez JL, Menezes A. "Software implementation of elliptic curve cryptography over binary fields," Koç ÇK, Paar C. (eds) Cryptographic hardware and embedded systems --- CHES 2000 Lecture Notes in Computer Science, vol. Springer, Berlin, Heidelberg.2000;1965:1-23. Available:https://doi.org/10.1007/3-540-44499-8_1
13. Al-Somani TF, Amin A. "Hardware implementations of gf (2m) arithmetic using normal basis," Journal of Applied Sciences. 2006;6: 1362-1372.
14. Guajardo J, Kumar SS, Paar C, Pelzl J. "Efficient software-implementation of finite fields with applications to cryptography," Appl. Math. 2006;93(1):3-32.
15. Koc CK, Acar T. "Montgomery multiplication in GF(2k)," Design, Codes and Cryptography. 1998;14(1): 57–69.
16. Itoh T, Tsujii S. "A fast algorithm for computing multiplicative inverses in GF(2m) using normal bases," Information and Computation. 1988;171-177. Available:http://www.sciencedirect.com/science/article/pii/0890540188900247
17. Rashidi B, Farashahi RR, Sayedi SM. "High-performance and high-speed implementation of polynomial basis Itoh–Tsujii inversion algorithm over GF(2m)," IET Information Security. 2017;11(2):66-77.
18. Hankerson D, Menezes A, Vanstone S. Guide to elliptic curve cryptography, New York, USA. Springer-Verlag; 2004.
19. NIST. "Digital Signature Standard (DSS)," Federal information processing standards publication, FIPS PUB. 2019;186-4:87-101.
20. Venturini YR. "Performance analysis of parallel modular multiplication algorithms for ECC in mobile devices," Revista de Sistemas de Informaçao da FSMA. 2014;13:57-67.
21. Rasmi M, Sokhon AA, Daoud MS, Al-Mimi H. "A survey on single scalar point multiplication algorithms forelliptic curves over prime fields," IOSR Journal of Computer Engineering (IOSR-JCE). 2016;18(2)V:31-47.
22. Rivain M. "Fast and regular algorithms for scalar multiplication over elliptic curves," [Online]; 2011. Available:https://eprint.iacr.org/2011/338.pdf
23. Karthikeyan E. "Survey of elliptic curve scalar multiplication algorithms," Int. J. Advanced Networking and Applications. 2012;4(2):1581-1590.
24. Pamula D. Arithmetic operators on GF(2m) for cryptographic applications: Performance-power consumption - security tradeoffs, Computer Arithmetic. Université Rennes 1, HAL Open Science; 2012.
25. López J, Dahab R. "Improved algorithms for elliptic curve arithmetic in GF(2n)"," Tavares S, Meijer H. (Eds.): Selected Areas in Cryptography SAC '98, LNCS. 1999;1556:201-212.




*Peer-review history:*
*The peer review history for this paper can be accessed here:*
*https://www.sdiarticle5.com/review-history/94995*