DOI: 10.2478/auom-2022-0003
An. Şt. Univ. Ovidius Constanţa **Vol. 30(1),2022, 43–56**

Different approach on elliptic curves mathematical models study and their applications

Ramzi Alsaedi, Abdelwahab Dhifli and Abdeljabbar Ghanmi

Abstract

In a research project in which a group of mathematical researchers is involved, it was necessary to create a system of nonlinear equations defined over a particular nonsupersingular elliptic space. This paper presents a part of the results obtained in this field, as well as the applications where the built models has been demonstrated their reliability.

1 Introduction

From their first definitions, the elliptic spaces models has been studied in order to create subspaces with applications in various other fields or in branches of mathematical study, in order to approximate some solutions. Where made multiple researches on particular elliptic spaces from their first descriptions, some of them on mathematics constructions ([1]), other with applications in cryptography ([8, 9, 10]) or even applications in some medical studies ([3, 4]). In our studies, we conceptualized subspaces that proved suitable to be used in the field of cryptography, building and demonstrating completeness for them.

Definition 1.1. *The Waierstrass form of an elliptic curve is given by:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

Key Words: Nonlinear system, Elliptic space, Elliptic curves.
2010 Mathematics Subject Classification: Primary 93C10; Secondary 11G05, 11G07.
Received:16.05.2021
Accepted: 31.07.2021

where $a_i \in K$ and K is the field over which the curve is defined.

The discriminant of this curve is: $\Delta = d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$ *where:* $d_2 = a_1 + 4a_2$*;* $d_4 = 2a_4 + a_1 a_3$*;* $d_6 = a_3^2 + 4a_6$*;* $d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$ *and* $\Delta \neq 0$*.*

In the case we have $K = F_p$ where $p > 3$ is a prime (1.1) can be simplified to: $E : y^2 = x^3 + ax + b$

The discriminant will then be $\Delta = -16(4a^3 + 27b^2)$. If $K = F_{2^m}$ the curve is given by: $E : y^2 = x^3 + ax + b$, the discriminant being $\Delta = b$.

2 Nonsupersingular Elliptic Curves Structure for particular fields

If the curve E is defined over a prime field F_p and we have a point $P(x, y) \in E$ then the inverse of it will be $-P(x, -y)$. If we want to compute $R(x_3, y_3) = P + Q$ where $P(x_1, y_1) \in E$ and $Q(x_2, y_2) \in E$ we have: $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, where λ is given by: $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$

To double a point $2P(x_3, y_3)$ we use the formulas: $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, where λ is given by:$\lambda = \frac{3x_1^2 + a}{2y_1}$. For the affine coordinates we replace x with x/z and y with y/z, where $z \neq 0$ obtaining the equation: $y^2 z = x^3 + axz^2 + bz^3$

To compute $P(x_1, y_1, z_1) + Q(x_2, y_2, z_2) = R(x_3, y_3, z_3)$ we have:

$$\begin{aligned}
\lambda_1 &= x_1 z_2^2 \\
\lambda_2 &= x_2 z_1^2 \\
\lambda_3 &= \lambda_1 - \lambda_2 \\
\lambda_4 &= y_1 z_2^3 \\
\lambda_5 &= y_2 z_1^3 \\
\lambda_6 &= \lambda_4 - \lambda_5 \\
\lambda_7 &= \lambda_1 + \lambda_2 \\
\lambda_8 &= \lambda_4 + \lambda_5 \\
z_3 &= z_1 z_2 \lambda_3 \\
x_3 &= \lambda_6^2 - \lambda_7 \lambda_3^2 \\
\lambda_9 &= \lambda_7 \lambda_3^2 - 2x_3 \\
y_3 &= (\lambda_9 \lambda_6 - \lambda_8 \lambda_3^3)/2
\end{aligned}$$

For doubling a point $2P(x_3, y_3, z_3)$ we use:

If the curve E is defined over a binary field F_{2^m} for a point $P(x, y)$ the inverse will be $-P(x, x + y)$. Addition and doubling are defined in the same way as on the prime curves. To obtain the projective coordinates we proceed

$$\begin{aligned}
\lambda_1 &= 3x_1^2 + az_1^4 \\
z_3 &= 2y_1z_1 \\
\lambda_2 &= 4x_1y_1^2 \\
x_3 &= \lambda_1^2 - 2\lambda_2 \\
y_3 &= \lambda_1(\lambda_2 - x_3) - 8y_1^4
\end{aligned}$$

as above. The inverse of a point $P(x, y, z)$ is $-P(x, x + y, z)$. To compute $P + Q = R$ we have:

$\lambda_1 = x_1z_2^2$; $\lambda_2 = x_2z_1^2$; $\lambda_3 = \lambda_1 + \lambda_2$; $\lambda_4 = y_1z_2^3$; $\lambda_5 = y_2z_1^3$; $\lambda_6 = \lambda_4 + \lambda_5$; $\lambda_7 = z_1\lambda_3$; $\lambda_8 = \lambda_6x_2 + \lambda_7y_2$; $z_3 = z_2\lambda_7$; $\lambda_9 = \lambda_6 + z_3$; $x_3 = az_3^2 + \lambda_6\lambda_9 + \lambda_3^2$; $y_3 = \lambda_9x_3 + \lambda_8\lambda_7^2$

And for doubling a point $2P$ we have: $z_3 = x_1z_1^2$, $x_3 = x_1^4 + bz_1^8$, $\lambda = z_3 + x_1^2 + y_1z_1$, $y_3 = x_1^4z_3 + \lambda x_3$. Arithmetic of elliptic curves can be further studied in [6].

2.1 Extracting the sets of cryptographic points

Not all the elliptic curves can be used in cryptography. A cryptosystem based on elliptic curves must have a high level of security. This level depends the most on the ECDLP (Elliptic Curve Discrete Logarithm Problem). For ECDLP to be infeasible the elliptic curve used must satisfy the following conditions [2]:

1. $|E(F_p)| = c \cdot l$ where $l > 2^{160}$ a prime and c a positive integer. $|E(F_p)|$ denotes the cardinal of the set of points on E over F_p.
2. $l \neq p$.
3. the order of the prime p in the multiplicative group $F_l^{\times}$ of F_l is at least $\lceil 2000/\log_2 p \rceil$.

These three conditions provide a high level of security. There were developed algorithms for resolving discrete logarithms with running time equal with the square root of the largest prime factor of the group order [17]. These algorithms cannot be applied to a cryprosystem which respects the first condition. In [11, 12] is described the anomalous curve attack. This attack consists in resolving the elliptic curve discrete logarithm problem for curves with the group order equal to the order of the finite field. The method uses Hensel's lemma and has low complexity. The second condition presented above makes this kind of attack impossible. In [15] the authors presented an attack which reduces the discrete logarithm problem in $E(F_p)$ to one in a finite extension field F_p. The third condition depends on the assumption that the DLP in a finite field which has a cardinal 2000-bit long is intractable.

The efficient of an elliptic curve cryptosystem is based on the arithmetic in F_p. So the efficiency is directly proportional with p. This means that $|E(F_p)|$ must be as small as possible. From the first condition we have $|E(F_p)| = c \cdot l$ where $l > 2^{160}$. So the efficienty depends on the cofactor c. The first condition becomes:

1. $|E(F_p)| = c \cdot l$ where $l > 2^{160}$ a prime and $c \leq 4$ a positive integer. $|E(F_p)|$ denotes the cardinal of the set of points on E over F_p.

3 Particular subspaces defined over nonsupersingular elliptic spaces and their applicability

For every elliptic curve cryptosystem we have to declare the domain parameters. We will work with a nonsupersingular elliptic curve E defined over a prime field. The domain parameters will be $(F, p, a_E, b_E, G, n, h)$ where F_p is the prime field, a_E, b_E define the curve $E : y^2 = x^3 + a_E x + b_E$, $G \in E$ is a point of order n (this means that n is the smallest positive number for which $nG = O$), $h = |E(F_p)|/n$ is the cofactor. To meet the above conditions it is recommended for $|E(F_p)|$ to be prime or $|E(F_p)| = h \cdot n$ where n is a large prime and $h \in \{1, 2, 3, 4\}$ [13], which where used on some recent applications ([14]).

3.1 Counting the Elliptic Curve's Points for the defined subspaces

To know the amount of points belonging to the elliptic curve we have to compute $|E(F_p)|$. Starting from the particular models ([9]), from derivations presented in some applications ([16]), basically all of them used a variant of an algorithm to count the points on an elliptic curve over a large field F_p. Initial version of it, made by Schoof's had a bigger running time and used Hasse's theorem on elliptic curves.

Theorem 3.1. *Hasse's Theorem. Variant for the case of nonsupersingular subspaces*

If E is an elliptic curve over the finite field F_p then: $|p+1-|E(F_p)|| \leq 2\sqrt{p}$

If we define $t = p + 1 - |E(F_p)|$ we have to compute $t \ mod \ N$ where $N > 4\sqrt{p}$. Schoof's algorithm computes this using small primes l_i where

$\prod l_i = N$. After computing t mod l_i we can find t using the Chinese Remainder Theorem. Knowing t we can then compute $|E(F_p)| = p + 1 - t$. To compute t mod l Schoof used the Frobenius endomorphism ϕ and division polynomials.

Theorem 3.2. *Frobenius endomorphism. Variant for the case of nonsupersingular subspaces*

The Frobenius endomorphism ϕ satisfies the following: $\phi^2 - t\phi + p = 0$ where $t = p + 1 + |E(F_p)|$

According to the theorem 3.2 we have the equation: $\phi^2 P + p_l P = t_l \phi P$ where $P(x, y) \in E(F_p)$. Here $p_l = p$ mod l and $t_l = t$ mod l. If we restrict to nontrivial l-torsion points (a tortion subgroup consists of all the elements of an abelian group that have finite order) we obtain: $(x^{p^2}, y^{p^2}) + \overline{p}(x, y) = \overline{t}(x^p, y^p)$ (2), where $\overline{x}$ is an unique integer such that $x = \overline{x}$ mod l. The above equation is valid because in a l-tortion subgroup the scalar multiplication has the property $pG = \overline{p}G$. Starting from (2) and applying division polynomials, Schoof's algorithm computes the value of $|E(F_p)|$. The reader can study the algorithm and its improvements made over time in [18].

Another variant of algorithm based on Hasse's theorem was developed for general applicability [10]. The algorithm computes a number $m \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ such that $mG = O$ where G is a random point from the curve $E : y^2 = x^3 + ax + b$. The algorithm is described below:

1. Compute $s \approx \sqrt[4]{p}$
2. Compute $G, 2G \dots sG$
3. Compute $Q = (2s + 1)P$ and $R = (p + 1)P$
4. Compute $R, R \pm Q, R \pm 2Q, \dots R \pm tQ$ where $t = \left[\frac{2\sqrt{p}}{2s+1}\right]$

The first three steps are known as baby steps while computing $R, R \pm Q \dots, R \pm tQ$ is the giant step. From Hasse's theorem we know that $R + iQ \quad i = 0, \pm 1, \pm 2, \dots, \pm t$ is equal with one from the points computed in second step. For this i we have: $R + iQ = jG \quad j \in \{0, \pm 1, \pm 2, \dots, \pm t\}$

The number m will be $m = p + 1 + (2s + 1)i - j$ which represents the cardinal of the elliptic curve points set. Variations, improvements and enhancements on this algorithm can be studied in [15].

3.2 Subspaces study

Next, we will exemplify some results from all the above methods on a particular subspace of a nonsupersingular elliptic curve. The domain parameters are

$(F, 7, 0, 1, G, n, h)$. The values for G, n, h will be computed after fixing a point on the curve. So, the elliptic curve is given by: $E : \ y^2 = x^3 + 1$ and the discriminant is: $\Delta = -16(4 * 0^3 + 27 * 1^2) \Rightarrow \Delta \neq 0$. The perfect squares in F_7 are $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$. Because we chose a small field, we can easily compute all the points from the curve:

$$\begin{array}{lclcl}
x = 0 & \Rightarrow & y^2 = 1 & \Rightarrow & (0,1)\ (0,6) \\
x = 1 & \Rightarrow & y^2 = 2 & \Rightarrow & (1,3)\ (1,4) \\
x = 2 & \Rightarrow & y^2 = 2 & \Rightarrow & (2,3)\ (2,4) \\
x = 3 & \Rightarrow & y^2 = 0 & \Rightarrow & (3,0) \\
x = 4 & \Rightarrow & y^2 = 2 & \Rightarrow & (4,3)\ (4,4) \\
x = 5 & \Rightarrow & y^2 = 0 & \Rightarrow & (5,0) \\
x = 6 & \Rightarrow & y^2 = 0 & \Rightarrow & (6,0)
\end{array}$$

The elliptic curve has $11 points + O = 12 points$. To compute operations in this field we need the inverses of the elements from F_7.

Definition 3.1. *Let x be an element from the finite field F_p then $x^{-1} \in F_p$ is the inverse of x if and only if: $x * x^{-1} = x^{-1} * x = 1(mod\ p)$*

The inverses from F_7 are emphasized in the table below:

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	**1**	3	5
3	0	3	6	2	5	**1**	4
4	0	4	**1**	5	2	6	3
5	0	5	3	**1**	4	6	3
6	0	6	5	4	3	2	**1**

If we take $P(4,3)$ and $Q(6,0)$ and we want to compute $R(x_3, y_3) = P + Q$ we have:

$$x_3 = \left(\frac{3-0}{4-6}\right)^2 - 4 - 6 = \frac{9}{4} - 4 - 6 = 2 * 4^{-1} - 4 - 6 = 2 * 2 - 4 - 6 = 1$$

$$y_3 = \left(\frac{3-0}{4-6}\right)(4-1) - 3 = \frac{-3}{2} * 3 - 3 = 4 * 2^{-1} * 3 - 3 = 4 * 4 * 3 - 3 = 3$$

So the result has the coordinates $R(1,3) \in E$.

We choose the parameter G with the coordinates $(1,3)$. To find the order n we have to find the smallest integer such that $nG = O$.
For $2P(x,y)$ we have:

$$x = \left(\frac{3 * 1^2 + 0}{2 * 3}\right)^2 - 2 * 1 = \frac{1}{4} - 2 = 4^{-1} - 2 = 2 - 2 = 0$$

$$y = \left(\frac{3 * 1^2 + 0}{2 * 3}\right)(1 - 0) - 3 = \frac{1}{2} - 3 = 2^{-1} - 3 = 4 - 3 = 1$$

So $2P(0,1) \in E$, for $3P(x,y)$ we have:

$$3P = P + 2P = (1,3) + (0,1)$$

$$x = \left(\frac{3-1}{1-0}\right)^2 - 1 - 0 = \frac{4}{1} - 1 = 4 - 1 = 3$$

$$y = \left(\frac{3-1}{1-0}\right)(1-3) - 3 = \frac{2}{1} * (-2) - 3 = -4 - 3 = 0$$

We obtained $3P(3,0) \in E$. For $4P$ we have:

$$4P = P + 3P = (1,3) + (3,0)$$

$$x = \left(\frac{3-0}{1-3}\right)^2 - 1 - 3 = \frac{9}{4} - 4 = 2 * 2 - 4 = 0$$

$$y = \left(\frac{3-0}{1-3}\right)(1-0) - 3 = \frac{-3}{2} - 3 = -3 * 4 - 3 = 6$$

While $4P(0,6) \in E$ for $5P$ we have:

$$4P = P + 4P = (1,3) + (0,6)$$

$$x = \left(\frac{3-6}{1-0}\right)^2 - 1 - 0 = \frac{9}{1} - 1 = 2 - 1 = 1$$

$$y = \left(\frac{3-6}{1-0}\right)(1-1) - 3 = -3 = 4$$

So $5P(1,4) \in E$ for $6P$ we have:

$$6P = P + 5P = (1,3) + (1,4)$$

$$x = \left(\frac{3-4}{1-1}\right)^2 - 1 - 1$$

We observe that the denominator is 0 which means that $6P = O$. Thus the order of $G(1,3)$ is $n = 6$. The cofactor is $h = |E(F_7)|/n = 12/6 = 2$. So the domain parameters are $(F, 7, 0, 1, G(1,3), 6, 2)$.

For the affine coordinates the initial curve $E: \ y^2 = x^3 + 1$ becomes $E: \ zy^2 = x^3 + z^3$. For this form of the curve the number of the points is much bigger. Because of that we will give some values to x and z to find some points from the curve for exemplifying the formulas presented in the first section.

$$\begin{array}{llllll}
x = 0 \ z = 0 & \Rightarrow & 0 * y^2 = 0 & \Rightarrow & (0,0,0) \ (0,1,0) \ (0,2,0) \ldots \\
x = 0 \ z = 1 & \Rightarrow & y^2 = 1 & \Rightarrow & (0,1,1) \ (0,6,1) \\
x = 1 \ z = 1 & \Rightarrow & y^2 = 2 & \Rightarrow & (1,3,1) \ (1,4,1) \\
x = 0 \ z = 2 & \Rightarrow & y^2 = 4 & \Rightarrow & (0,2,2) \ (0,5,2)
\end{array}$$

If we choose $P(1,3,1) + Q(0,6,1) = R(x,y,z)$ we have:

$$\begin{array}{lll}
\lambda_1 & = & 1 * 1^2 = 1 \\
\lambda_2 & = & 0 * 1^2 = 0 \\
\lambda_3 & = & 1 - 0 = 1 \\
\lambda_4 & = & 3 * 1^3 = 3 \\
\lambda_5 & = & 6 * 1^3 = 6 \\
\lambda_6 & = & 3 - 6 = 4 \\
\lambda_7 & = & 1 + 0 = 1 \\
\lambda_8 & = & 3 + 6 = 2 \\
z_3 & = & 1 * 1 * 1 = 1 \\
x_3 & = & 4^2 - 1 * 1^2 = 1 \\
\lambda_9 & = & 1 * 1^2 - 2 * 1 = 6 \\
y_3 & = & (6 * 4 - 2 * 1^3)/2 = 22/2 = 4
\end{array}$$

So $P + Q$ is $R(1,4,1) \in E$. If we want to double the point P we have:

$$\begin{array}{lll}
\lambda_1 & = & 3 * 1^2 + 0 * 1^4 = 3 \\
z_3 & = & 2 * 3 * 1 = 6 \\
\lambda_2 & = & 4 * 1 * 3^2 = 1 \\
x_3 & = & 3^2 - 2 * 1 = 0 \\
y_3 & = & 3(1 - 0) - 8 * 3^4 = 3 - 648 = 1
\end{array}$$

Thus $2P(0,1,6)$ which is on the elliptic curve E because:

$$6 * 1^2 = 0^3 + 6^3 \Leftrightarrow 6 = 216(mod\ 7)$$

3.3 Optimisations over the particular subspaces

If we look at the problem from a different point of view, we can start from the form of such an integral

$$\int \frac{dx}{\sqrt{4x^3 - h_2 x - h_3}} \tag{3.1}$$

The inverse function of such an integral is called elliptic function. Let be two constants α_1 and α_2, a function and a double periodic function over R then Weierstrass function will be of the type

$$(\gamma')^2 = 4\gamma^3 - \alpha_1\gamma - \alpha_2 \tag{3.2}$$

This pair (γ, γ') will define a point on the curve

$$y^2 = 4x^3 - \alpha_1 x - \alpha_2 \tag{3.3}$$

making an elliptic curve.

Definition 3.2. *Let be $p > 3$ a prime integer. The elliptic curve $y^2 = x^3 + \alpha_1 x + \alpha_2$, defined over Z_p is the set of solutions $(x, y) \in Z_p \times Z_p$ to the congruence*

$$y^2 \equiv x^3 + \alpha_1 x + \alpha_2 \,(mod\, p) \tag{3.4}$$

where $\alpha_1, \alpha_2 \in Z_p$ are constants such that $4\alpha_1^3 + 27\alpha_2^2 \not\equiv 0 \,(mod\, p)$ together with a special point $\mathfrak{O}$ called the point at infinity.

As already described in section 2 the main problems are to define the addition of two points in such a field and to make multiplications by a given integer to a point on the elliptic curve. Let be A_1 and A_2 two points from the elliptic curve. The adding problem of these points can be split in two categories:

- $x_1 = x_2$ and $y_1 = y_2$
- other cases

Lemma 3.1. *Let E denote an elliptic curve given by*

$$E : Y_2 + \alpha_1 XY + \alpha_3 Y = X^3 + \alpha_2 X^2 + \alpha_4 X + \alpha_6 \tag{3.5}$$

and let be $A_1 = (x_1, y_1)$ and $A_2 = (x_2, y_2)$ two points on the curve. Then

$$-A_1 = (x_1, -y_1 - \alpha_1 x_1 - \alpha_3) \tag{3.6}$$

Set

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \ \gamma = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \tag{3.7}$$

where x_1, x_2 satisfy the condition $x_1 \neq x_2$ and, from this point we will have

$$\lambda = \frac{3x_1^2 + 2\alpha_2 x_1 + \alpha_4 - \alpha_1 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3},\ \gamma = \frac{-x_1^3 + \alpha_4 x_1 + 2\alpha_6 - \alpha_3 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3}. \tag{3.8}$$

In case of equality between x_1 and x_2 and $A_2 \neq -A_1$ the sum of these two points will be the point A_3 with the following coordinates:

$$x_3 = \lambda^2 + \alpha_1 \lambda - \alpha_2 - x_1 - x_2,\ y_3 = -(\lambda + \alpha_1)x_3 - \gamma - \alpha_3 \tag{3.9}$$

Thus we will have

1. $x_2 = x_1$ and $y_2 = y_1$. Then $A_1 + A_2 = \mathfrak{O}$
2. Otherwise $A_1 + A_2 = B$, $B(x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1 \tag{3.10}$$

and

$$\lambda = \left\{ \begin{array}{l} (y_2 - y_1)(x_2 - x_1)^{-1}, A_1 \neq A_2; \\ (3x_1^2 + a)(2y_1)^{-1}, A_1 = A_2; \end{array} \right. \tag{3.11}$$

In practice there are used the elliptic curves defined over a finite field F_q, which means that the study will be made on an abelian group. Let be s the number of points on an elliptic curve E, defined over F_q. Then $s = \#E(F_q) = q+1-t$, where $\#E(F_q)$ is named trace of Frobenius at q. Thus we can define Frobenius endomorphism as being

$$\varphi = \left\{ \begin{array}{l} E(\overline{F}_q) \longrightarrow E(\overline{F}_q) \\ (x, y) \longrightarrow (x^q, y^q) \\ \mathfrak{O} \longrightarrow \mathfrak{O} \end{array} \right. \tag{3.12}$$

Lemma 3.2. *Let E be an elliptic curve over F_q and m is a prime which divides $\#E(F_q)$ but which does not divide $q - 1$ and $m \neq char(F_q)$. Then $E(F_{q^k})$ contains the m^2 points of order m iff m divides $q^k - 1$*

According to [18] we will define Weil pairing as being $E(m) \times E(m) \longrightarrow \gamma_m$ where γ_m is the group of mth roots of unity in $\overline{K}$. Thus, let be $B_1, B_2 \in E[m]$ and we choose a function g in E whose divisor satisfies

$$div(g) = \sum_{D \in E[m]} (B_1' + D) - (D) \tag{3.13}$$

with $B' \in E(\overline{K})$ such that $[m]B' = B$. In this case, we define e_m as:

$$e_m = \left\{ \begin{array}{l} E[m] \times E[m] \longrightarrow \gamma_m \\ (B_1, B_2) \longrightarrow \frac{g(X+B_1)}{g(X)} \end{array} \right. \tag{3.14}$$

In the case of the implementation in computing systems of a subfield curve, of the type F_{q^n}, n must be greater than 1 and the coefficients from F_q. We will define, like in [14], as a new addition method (and subsequently multiplication method by an integer) of two points on the elliptic curve using Frobenius Expansion. In equation (16) φ must satisfies equation

$$\varphi^2 - [t]\varphi + [q] = [0] \tag{3.15}$$

4 Applicability of the chosen subspaces

From the previous conditions follows that the subspaces can be grouped by their order of computational complexity. In order to describe the applicability we choose M_i as the signing member from the group. He first choses a random value $\alpha \in Z_q$. Then it encrypts his own key y_i by computing $A = z^\alpha$ and $B = y_i g^\alpha$. He computes $(c_1, \ldots, c_n, s_c, \ldots, s_n)$ from $SEQDL_1^n(z, g, A, \frac{B}{y_1}, \ldots, A, \frac{B}{y_n}, message)$. Finally, it computes the pair $(\tilde{c}, \tilde{s} = SKDL(g, B, message))$.

So it become the group signature, $(A, B, c_1, \ldots, c_n, s_c, \ldots, s_n, \tilde{c}, \tilde{s})$. To prove that the completeness of the model we discuss the last two chosen parameters, which are in fact, the entities signatures. So, the first signature proves that the member has encrypted a key from Y. To better understand this we take M_3 from a group of 5 members to be the one who will sign the message. So the first signature will look like this:

$$(c_1, \ldots c_5, s_1 \ldots s_5)$$

is $SEQDL_1^5(z, g, A, \frac{B}{y_1}, \ldots, A, \frac{B}{y_5}, message)$. So we have

$SEQDL_1^5(z, g, A, \frac{B}{y_1}, A, \frac{B}{y_2}, A, \frac{B}{y_3}, A, \frac{B}{y_4}, A, \frac{B}{y_5},\ message)$.

$SEQDL_1^5(z, g, A, \frac{y_3 g^\alpha}{y_1}, A, \frac{y_3 g^\alpha}{y_2}, A, \frac{y_3 g^\alpha}{y_3}, A, \frac{y_3 g^\alpha}{y_4},\ A, \frac{y_3 g^\alpha}{y_5}, message)$.

$SEQDL_1^5(z, g, z^\alpha, \frac{B}{y_1}, z^\alpha, \frac{B}{y_2}, \underline{z^\alpha, g^\alpha}, z^\alpha, \frac{B}{y_4}, z^\alpha, \frac{B}{y_5},\ message)$.

The second signature proves the knowledge of the parameters, and also the chosen subspace for it. From these, we have $(\tilde{c}, \tilde{s} = SKDL(g, B, message))$ and $(\tilde{c}, \tilde{s} = SKDL(g, y_3 g^\alpha, message))$. To open a group signature the manager has first to decrypt (A, B).

$$\begin{aligned} \frac{B}{A^{\omega^{-1}}} &= \frac{y_3 g^\alpha}{z^{\alpha\omega^{-1}}} \\ &= \frac{y_3 g^\alpha}{g^{\omega\alpha\omega^{-1}}} \end{aligned}$$

$$= \quad y_3$$

From this it is deducted: $SEQDL(g, z, B/(y_3), A, M_3)$ for $SEQDL(g, z, y_3 g^\alpha/(y_3), z^\alpha, M_3)$ and $SEQDL(g, z, g^\alpha, z^\alpha, M_3)$.

It represents a less part of the computing complexity of the original way of determining the parameters of the previous model ([11]) and the applicability of these research will increase the accuracy of the results from ([6]), which use the initial results.

5 Conclusions

To simplify the scalar multiplications that we had to compute for all the above examples we used the binary representation, but also the ideea presented in [9]. Having already the values for several multiples of the point $G(1,3)$ we used them to compute bigger multiples with fewer operations or their way implemented in medical studies ([5, 7]). We only computed (4+2) operations, so with 25% less. For $G_3 = 7G$ we already knew $5G$ and $2G$ and so we had only two operations (one for x and one for y), like in ([1]). The classic way implies 14 operations because $7G = (((((2G + G) + G) + G) + G) + G) + G$, so the improvement on computational complexity is obvious. On the current studies we research a way to prove the unicity of parameters implied on the nonlinear equations used on the general model, which will have applicability for supersingular elliptic curves.

Acknowledgments: This work was funded by the University of Jeddah, Saudi Arabia, under grant No. UJ-02-008-ICGR. The authers, therefore, acknowledge with thanks the University technical and financial support.

References

[1] Henri Cohen, Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC 2006.

[2] Jean Sebastien Coron, David Lefranc, Guillaume Poupard, A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis, Cryptographic Hardware and Embedded Systems, CHES 2005, Springer Berlin/Heidelberg, 2005.

[3] Antonescu Elisabeta, Bota Gabriela, Serb Bogdan, Duicau Lavinia, Study of the Total Serum Concentration of Serum Ionized Magnesium in Children and Adolescents from Sibiu Area, Revista de chimie, **69** (2018), no. 12, 3389–3392.

[4] Duica Lavinia, Depression - multiple psychopathological faces (a case report), Proceedings of the International Conference on Mental Health - Psychology, Medicine and Anthropology for Life Quality, Romania, 2016, 59–62.

[5] Silisteanu Sinziana, Antonescu, Elisabeta, Duica Lavinia, The importance of balance and postural control in the recovery of stroke patients, Balneo Research Journal, **11** (2020), no. 3, 372–378.

[6] Duica Lavinia, The use of the internet - professional development or internet addiction in medical students, Journal of Educational Sciences & Psychology, **7** (2017), no. 2, 59–64.

[7] Mutica M., Ciubara Anamaria, Duica Lavinia, Alexandru D., Plesea Condratovici, Pirlog Mihail, Elderly schizophrenic patients - clinical and social correlations, European Neuropsychopharmacology, **26** (2016), no. 2, 5512-5512.

[8] Constantinescu Nicolae, Security System Vulnerabilities, Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences, **13** (2012), no. 2, 175–179.

[9] Stephanides George, Constantinescu Nicolae, Cosulschi Mirel, Gabroveanu Mihai, RSA-padding signatures with attack studies, WEBIST 2006, 97–1000.

[10] Ticleanu Oana, Constantinescu Nicolae, Intelligent data retrieval with hierarchically structured information, KES IIMS 2013, 345–351.

[11] Stephanides George, Constantinescu Nicolae, The GN-authenticated key agreement, Applied Mathematics and Computation, **170** 2015, no. 1, 531–544.

[12] Emil Simion, Nicolae Constantinescu, Complexity Computations in Code Cracking Problems, Concurrent Engineering in Electronic Packaging, IEEE Communication, ISSE 2001, 225–232.

[13] Oana Ticleanu, Differential operators over particular elliptic curves spaces with cryptographic applications. E. Journal of Differential Equations, **2015**, no.303, 1–5.

[14] Oana Ticleanu, Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography. E. Journal of Differential Equations, **2015**, no. 214, 1–9.

[15] Alin Golumbeanu, Oana Ticleanu, Elliptic Curves Differentiation with Application to Group Signature Scheme, E. Journal of Differential Equations, **2017**, no. 237, 1–21.

[16] Nicolae Constantinescu, Oana Ticleanu, Alin Golumbeanu, Nonlinieari-ties on Cryptographic Shift Registers, Annals of the University of Craiova, Mathematics and Computer Science Series, **43** 2016, no. 1, 27–32.

[17] Chaum David, Ernest Van Heyst, Group signatures, Advances in Cryptology Eurocrypt '91, **547** , 257–265.

[18] Camenisch John, Stadler Michael, Efficient group signatures schemes for large groups, Advances in Cryptology-Crypto 1997, **1294**, 410–424.

Ramzi Alsaedi,
Department of Mathematics,
King Abdulaziz University,
Faculty of Sciences, P.O. Box 80203, Jeddah 21589, Saudi Arabia.
Email: ramzialsaedi@yahoo.co.uk.
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: rsalsaedi@uj.edu.sa.

Abdelwahab Dhifli,
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: amdhifli@uj.edu.sa.

Abdeljabbar Ghanmi,
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: aaalghanmy1@uj.edu.sa.