Gulf Journal of Mathematics
Vol 6, Issue 4 (2018) 72-78

ECC OVER THE RING $\frac{\mathbb{F}_{2^d}[X]}{(X^2)}$ BY USING A PASSWORD

A. TADMORI [1*], A. CHILLALI [2] AND M. ZIANE [3]

Abstract. In this work, we will present an example of encryption and decryption, by using the elliptic curve defined over the ring $\mathbf{A_2} = \mathbb{F}_{2^d}[\varepsilon]$, where d is a positive integer and $\varepsilon^2 = 0$. The motivation for this work came from the observation that communications, industrial automation and many more. For majority of these applications, security is a vital issue. Cryptography plays an important role in providing data security. In a first time, we describe these curves defined over this ring. Then, we study the algorithmic properties by proposing effective implementations for representing the elements and the group law. In other we give an example of encrypted message with a secret key.

1. Introduction

Let d be an integer, we consider the quotient ring

$$\mathbf{A_2} = \frac{\mathbb{F}_{2^d}[X]}{(X^2)},$$

where $\mathbb{F}_{2^d}$ is the finite field of order 2^d.
Then the ring $\mathbf{A_2}$ is identified to the ring $\mathbb{F}_{2^d}[\varepsilon]$ with $\varepsilon^2 = 0$, ie:

$$\mathbf{A_2} = \{\, a_0 + a_1 \cdot \varepsilon \mid a_0, a_1 \in \mathbb{F}_{2^d} \,\}.$$

We consider the elliptic curve over the ring $\mathbf{A_2}$ which is given by equation:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3. \tag{1.1}$$

where a, b are in $\mathbf{A_2}$ and b is invertible in $\mathbf{A_2}$, see [4] and [3].

2. Notations

Lets a,b $\in \mathbf{A_2}$ such that b is invertible in $\mathbf{A_2}$. We denote the elliptic curve over $\mathbf{A_2}$ by $\mathbf{E}_{a,b}(\mathbf{A_2})$ and we write:

$$\mathbf{E}_{a,b}(\mathbf{A_2}) = \{\, [X : Y : Z] \in \mathbb{P}_2(\mathbf{A_2}) \mid Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \,\}.$$

If $b_0 \in \mathbb{F}_{2^d} \setminus \{0\}$ and $a_0 \in \mathbb{F}_{2^d}$, we also write:

$$\mathbf{E}_{a_0,b_0}(\mathbb{F}_{2^d}) = \{\, [X : Y : Z] \in \mathbb{P}_2(\mathbb{F}_{2^d}) \mid Y^2Z + XYZ = X^3 + a_0X^2Z + b_0Z^3 \,\}.$$

Date: Received: Dec 2, 2018
* Corresponding author.
2010 *Mathematics Subject Classification.* 11Y40.
Key words and phrases. Finite Ring, Elliptic curve, Cryptograpy, Binary codes.

3. Classification of elements of $\mathbf{E}_{a,b}(\mathbf{A_2})$

Let $[X : Y : Z] \in \mathbf{E}_{a,b}(\mathbf{A_2})$, where X, Y and Z are in $\mathbf{A_2}$. We have two cases for Z:

- Z invertible: then, $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1]$ hence, we take just $[X : Y : 1]$.
- Z non invertible: so, $Z = z_1\varepsilon$ see [3], in this case we have two cases for Y.

- if Y invertible: then, $[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}]$ so, we just take $[X : 1 : z_1\varepsilon] \in \mathbf{E}_{a,b}(\mathbf{A_2})$ then, verifies the equation (1.1). We write:

$$a = a_0 + a_1\varepsilon$$
$$b = b_0 + b_1\varepsilon$$
$$X = x_0 + x_1\varepsilon$$

We have;

$$z_1\varepsilon + (x_0 + x_1\varepsilon)\cdot z_1\varepsilon = (x_0 + x_1\varepsilon)^3 + (a_0 + a_1\varepsilon)\cdot(x_0 + x_1\varepsilon)^2\cdot z_1\varepsilon + (b_0 + b_1\varepsilon)\cdot z_1^3\varepsilon^3,$$

which implies that

$$z_1\varepsilon + (x_0 z_1\varepsilon) = x_0^3 + (x_0^2 x_1 + a_0 x_0^2 z_1)\varepsilon$$

so,

$$z_1\varepsilon + x_0 z_1\varepsilon = x_0^3 + (x_0^2 x_1 + a_0 x_0^2 z_1)\varepsilon$$

then,

$$(z_1 + x_0 z_1)\cdot\varepsilon = x_0^3 + (x_0^2 x_1 + a_0 x_0^2 z_1)\varepsilon$$

since $(1, \varepsilon)$ is a basis of the vector space $\mathbf{A_2}$ over $\mathbb{F}_{2^d}$ then, $x_0 = 0$ so, $X = x_1\varepsilon$ and $z_1\varepsilon = 0$ (ie $z_1 = 0$) hence, $[X : 1 : z_1\varepsilon] = [x_1\varepsilon : 1 : 0]$.

- if Y non invertible: then, we have $Y = y_1\varepsilon$ so, $x = x_0 + x_1\varepsilon$ is invertible hence, we take $[X : Y : Z] \sim [1 : y_1\varepsilon : z_1\varepsilon]$, thus $1 + a.z_1\varepsilon = 0$ ie: $1 + a_0.z_1\varepsilon = 0$, which is absurd

Proposition 3.1. *Every element of* $\mathbf{E}_{a,b}(\mathbf{A_2})$ *is of the form* $[X : Y : 1]$ *or* $[x\varepsilon : 1 : 0]$, *where* $x \in \mathbb{F}_{2^d}$ *and we write*

$$\mathbf{E}_{a,b}(\mathbf{A_2}) = \{\,[X : Y : 1] \in \mathbb{P}_2(\mathbf{A_2}) \mid Y^2 + XY = X^3 + aX^2 + b\,\} \bigcup \{\,[x\varepsilon : 1 : 0] \mid x \in \mathbb{F}_{2^d}\,\}.$$

- we consider the canonical projection π defined by:

$$\pi : \mathbf{A_2} \longrightarrow \mathbb{F}_{2^d}$$
$$x_0 + x_1\varepsilon \longmapsto x_0$$

π is a morphism of rings.

- let π_2 the mapping defined by:

$$\mathbf{E}_{a,b}(\mathbf{A_2}) \xrightarrow{\pi_2} \mathbf{E}_{a_0,b_0}(\mathbb{F}_{2^d})$$
$$[X : Y : Z] \longmapsto [\pi(X) : \pi(Y) : \pi(Z)]$$

Theorem 3.2. *Lets* $\mathbf{P} = [X_1 : Y_1 : Z_1]$ *and* $\mathbf{Q} = [X_2 : Y_2 : Z_2]$ *two points in* $\mathbf{E}_{a,b}(\mathbf{A_2})$, *and* $\mathbf{P} + \mathbf{Q} = [X_3 : Y_3 : Z_3]$.

- *if* $[\pi(X_1) : \pi(Y_1) : \pi(Z_1)] = [\pi(X_2) : \pi(Y_2) : \pi(Z_2)]$, *then:*
  $X_3 = X_1Y_1Y_2^2+X_2Y_1^2Y_2+X_2^2Y_1^2+X_1X_2^2Y_1+aX_1^2X_2Y_2+aX_1X_2^2Y_1+aX_1^2X_2^2+bX_1Y_1Z_2^2+bX_2Y_2Z_1^2+bX_1^2Z_2^2+bY_1Z_2^2Z_1+bY_2Z_1^2Z_2+bX_1Z_2^2Z_1$
  $Y_3 = Y_1^2Y_2^2+X_2Y_1^2Y_2+aX_1X_2^2Y_1+a^2X_1^2X_2^2+bX_1^2X_2Z_2+bX_1X_2^2Z_1+bX_1Y_1Z_2^2+bX_1^2Z_2^2+abX_2^2Z_1^2+abX_1^2Z_2^2+bY_1Z_1Z_2^2+bX_1Z_1Z_2^2+abX_1Z_1Z_2^2+abX_2Z_1^2Z_2+b^2Z_1^2Z_2^2$
  $Z_3 = X_1^2X_2Y_2+X_1X_2^2Y_1+Y_1^2Y_2Z_2+Y_1Y_2^2Z_1+X_1^2X_2^2+Y_1^2X_2Z_2+X_1^2Y_2Z_2+aX_1^2Y_2Z_2+aX_2^2Y_1Z_1+X_1^2X_2Z_2+aX_1X_2^2Z_1+bY_1Z_1Z_2^2+bY_2Z_1^2Z_2+bX_1Z_1Z_2^2$
- *if* $[\pi(X_1) : \pi(Y_1) : \pi(Z_1)] \neq [\pi(X_2) : \pi(Y_2) : \pi(Z_2)]$, *then:*
  $X_3 = X_1Y_2^2Z_1+X_2Y_1^2Z_2+X_1^2Y_2Z_2+X_2^2Y_1Z_1+aX_1^2X_2Z_2+aX_1X_2^2Z_1+bX_1Z_1Z_2^2+bX_2Z_1^2Z_2$
  $Y_3 = X_1^2X_2Y_2+X_1X_2^2Y_1+Y_1^2Y_2Z_2+Y_1Y_2^2Z_1+X_1^2Y_2Z_2+X_2^2Y_1Z_1+aX_1^2Y_2Z_2+aX_2^2Y_1Z_1+aX_1^2X_2Z_2+aX_1X_2^2Z_1+bY_1Z_1Z_2^2+bY_2Z_1^2Z_2+bX_1Z_1Z_2^2+bX_2Z_1^2Z_2$
  $Z_3 = X_1^2X_2Z_2+X_1X_2^2Z_1+Y_1^2Z_2^2+Y_2^2Z_1^2+X_1Y_1Z_2^2+X_2Y_2Z_1^2+aX_1^2Z_2^2+aX_2^2Z_1^2$

Proof. Using the explicit formulas in W.Bosma and H.Lenstra article , see [15], we prove the theorem. □

Remark 3.3.
- with this theorem we prove that the mapping π_2 is a surjective morphism of groups.
- $(\mathbf{E}_{a,b}(\mathbf{A_2}), +)$ is a group of unity $[0 : 1 : 0]$, and the opposite of element $[X : Y : Z]$ is $[X : X + Y : Z]$.

4. Cryptography based on a password

Let $\mathbf{E}_{a,b}(\mathbf{A_2})$ an elliptic curve over A_2 and an irreducible polynomial $R(X) = 1 + X + X^3$ in $\mathbb{F}_2[X]$. $R(X)$ have not roots in the $\mathbb{F}_2$ because $R(0) = 1$, $R(1) = 1$ but there exist an α where $R(\alpha) = 0$ in $\mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{(R(X))}$, so $(1, \alpha, \alpha^2)$ is a basis of the vector space $\mathbb{F}_8$ over $\mathbb{F}_2$.

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + 1, \alpha^2 + \alpha + 1\}$$

• Lets

$$a = 1 + \alpha$$
$$b = 1 + \alpha^2\varepsilon$$

so;

$$\mathbf{E}_{a,b}(\mathbb{F}_8[\varepsilon]) : Y^2 + XY = X^3 + (1 + \alpha)X^2 + (1 + \alpha^2\varepsilon).$$

Let $P \in \mathbf{E}_{a,b}(\mathbb{F}_8[\varepsilon])$ of order l, we will use the subgroup $< P >$ of $\mathbf{E}_{a,b}(\mathbb{F}_8[\varepsilon])$ to encrypt messages, and we denote $G =< P >$.

4.1. **Coding of elements of G.** We will give a code to each element $Q = mP$ where $m \in \{1, 2, .., l\}$ defined as following:
Assume $Q = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : Z]$ where $x_i, y_i \in \mathbb{F}_8$ for $i = 0$ or 1 and $Z = 0$ or 1, we set:

$$x_i = c_{0i} + c_{1i}\alpha + c_{2i}\alpha^2$$
$$y_i = d_{0i} + d_{1i}\alpha + d_{2i}\alpha^2$$

where α is a primitive root of an irreducible polynomial of degree 3 over $\mathbb{F}_2$ and $c_{ij}, d_{ij} \in \mathbb{F}_2$, then we code Q as it follows:

- if $Z = 1$ then;

$$Q = c_{00}c_{10}c_{20}1c_{01}c_{11}c_{21}1d_{00}d_{10}d_{20}1d_{01}d_{11}d_{21}1$$

- if $Z = 0$ then;

$$Q = 0000c_{01}c_{11}c_{21}0d_{00}d_{10}d_{20}00000$$

4.2. **Example.**

$$a = 1 + \alpha$$

$$b = 1 + \alpha^2\varepsilon$$

The elliptic curve $\mathbf{E}_{a,b}(\mathbb{F}_8[\varepsilon])$ has 112 elements:
$\{[(\alpha^2+\alpha+1)\varepsilon : 1 : 0], [(\alpha^2+1)\varepsilon : 1 : 0], [(1+\alpha)\varepsilon : 1 : 0], [(\alpha^2+\alpha)\varepsilon : 1 : 0], [\alpha^2\varepsilon : 1 : 0], [\alpha\varepsilon : 1 : 0], [\varepsilon+\alpha^2+1 : \alpha\varepsilon+\alpha : 1], [\alpha^2+\alpha : (\alpha^2+\alpha+1)\varepsilon : 1], [\alpha^2\varepsilon : \varepsilon+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+1 : (\alpha^2+\alpha)\varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2 : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : 1], [(\alpha^2+\alpha)\varepsilon+1+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha^2+1 : \alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha+1 : \varepsilon+1 : 1], [1+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2 : (\alpha^2+1)\varepsilon+\alpha^2+1 : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha+1 : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon+1+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha\varepsilon+\alpha^2+1 : \varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+1)\varepsilon+1+\alpha : (\alpha^2+\alpha)\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+\alpha^2+\alpha : 0 : 1], [\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2 : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon+\alpha^2+1 : (\alpha^2+\alpha+1)\varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+\alpha)\varepsilon : 1], [(\alpha^2+\alpha+1)\varepsilon+1+\alpha : \varepsilon+\alpha^2 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+1)\varepsilon+1+\alpha : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\varepsilon+\alpha^2 : \alpha\varepsilon+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : \alpha\varepsilon+1 : 1], [\alpha^2\varepsilon : \alpha\varepsilon+1 : 1], [\varepsilon+\alpha^2+\alpha : \varepsilon : 1], [(1+\alpha)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha^2\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : \alpha^2\varepsilon+1 : 1], [(1+\alpha)\varepsilon+\alpha^2 : \alpha^2\varepsilon+1 : 1], [\alpha^2\varepsilon : \alpha^2\varepsilon+1 : 1], [\alpha^2+\alpha+1 : (\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon : 1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2 : 1 : 1], [\varepsilon+\alpha, (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+1+\alpha : \varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : (1+\alpha)\varepsilon : 1], [\varepsilon+\alpha^2+\alpha+1 : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [\varepsilon+1+\alpha : \alpha\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha+1 : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha+1 : 1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [\alpha^2 : \varepsilon+\alpha^2+1 : 1], [(1+\alpha)\varepsilon+1+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha^2+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [\varepsilon+\alpha^2+\alpha : \alpha^2+\alpha : 1], [\alpha\varepsilon+1+\alpha : \alpha^2+\alpha+1 : 1], [\alpha^2 : \varepsilon+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+\alpha+1)\varepsilon+1 : 1], [\alpha^2\varepsilon : (\alpha^2+\alpha+1)\varepsilon+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+1 : (\alpha^2+1)\varepsilon+\alpha : 1], [\varepsilon+\alpha^2 : (1+\alpha)\varepsilon+\alpha^2+1 : 1], [\varepsilon+1+\alpha : (1+\alpha)\varepsilon+\alpha^2 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2 : (\alpha^2+\alpha)\varepsilon+\alpha^2+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+1)\varepsilon : 1], [\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+1)\varepsilon+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : \alpha^2\varepsilon+\alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha : \alpha\varepsilon : 1], [(\alpha^2+\alpha)\varepsilon+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha : \varepsilon+\alpha^2+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha+1 : \alpha^2+\alpha : 1], [\alpha^2+\alpha+1 : (\alpha^2+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon : (\alpha^2+\alpha)\varepsilon+1 : 1] , [\alpha^2\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+1+\alpha : \alpha\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha^2 : \alpha^2+1 : 1], [\alpha\varepsilon+\alpha : \alpha^2+\alpha : 1], [(1+\alpha)\varepsilon+1+\alpha : \alpha^2\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha : \varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon+\alpha^2 : \alpha\varepsilon+\alpha^2+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+1)\varepsilon+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2 : \alpha^2\varepsilon+\alpha^2+1 : 1], [\alpha^2\epsilon : (\alpha^2+1)\varepsilon+1 : 1], [\alpha^2\varepsilon+\alpha : (\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : 1], [1+\alpha :$

$(\alpha^2+1)\varepsilon+\alpha^2:1],[(\alpha^2+\alpha+1)\varepsilon+1+\alpha:(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1:1],[\alpha^2\varepsilon+\alpha^2:(\alpha^2+\alpha)\varepsilon+1:1],[\alpha^2+1:(1+\alpha)\varepsilon+\alpha:1],[(\alpha^2+1)\varepsilon+\alpha^2+\alpha:\alpha^2\varepsilon:1],[\alpha^2\varepsilon+1+\alpha:\alpha^2:1],[0:1:0],[\alpha:\alpha\varepsilon+\alpha^2:1],[\varepsilon+\alpha:\alpha\varepsilon+\alpha^2:1],[(\alpha^2+\alpha+1)\varepsilon+\alpha:\alpha\varepsilon+\alpha^2:1],[(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1:\varepsilon+\alpha^2+\alpha:1],[\alpha^2\varepsilon+\alpha^2+\alpha:(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha:1],[\alpha\varepsilon+\alpha^2:(\alpha^2+\alpha+1)\varepsilon+1:1],[\varepsilon:1:0],[(\alpha^2+1)\varepsilon+\alpha^2:(\alpha^2+1)\varepsilon+1:1]\}$

Let; $P=[\alpha:\alpha+\alpha^2+\alpha\varepsilon:1]=0101000101110101$. We also attach any element $Q\in G$ a letter of the alphabet or a punctuation sign and we assemble the results in the following table:

	mP	*code of mP*	*symbol*
1	$[\alpha:\alpha+\alpha^2+\alpha\varepsilon:1]$	0101000101110101	a
2	$[1+\alpha+\varepsilon:\alpha^2+(1+\alpha)\varepsilon:1]$	1101100100111101	b
3	$[\alpha^2+\alpha\varepsilon:1+\alpha^2+(\alpha^2+1)\varepsilon:1]$	1101011100111111	c
4	$[1+\alpha+\alpha^2+(1+\alpha)\varepsilon:\alpha+\alpha^2:1]$	1111110101110001	d
5	$[\alpha+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:(1+\alpha)\varepsilon:1]$	0111111100011101	e
6	$[1+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:\alpha+\alpha^2\varepsilon:1]$	1011111101010011	f
7	$[\alpha^2\varepsilon:1+(1+\alpha^2)\varepsilon:1]$	0001001110011011	g
8	$[1+\alpha^2+(1+\alpha^2)\varepsilon:1+\alpha+\alpha^2+(1+\alpha)\varepsilon:1]$	1011101111111101	h
9	$[\alpha+\alpha^2+\alpha\varepsilon:\alpha+\alpha^2+\alpha\varepsilon:1]$	0111010101110101	i
10	$[1+\alpha+\alpha^2+\alpha\varepsilon:1:1]$	1111010110010001	j
11	$[\alpha^2+\alpha^2\varepsilon:1+(\alpha+\alpha^2)\varepsilon:1]$	0011001110010111	k
12	$[1+\alpha+(\alpha+\alpha^2)\varepsilon:1+\alpha+\alpha^2+\varepsilon:1]$	1101011111111001	l
13	$[\alpha+(1+\alpha)\varepsilon:\alpha^2+\alpha\varepsilon:1]$	0101110100110101	m
14	$[\alpha^2\varepsilon:1:0]$	0000001010000000	n
15	$[\alpha+(1+\alpha)\varepsilon:\alpha+\alpha^2+\varepsilon:1]$	0101110101111001	o
16	$[1+\alpha+(\alpha+\alpha^2)\varepsilon:\alpha^2+(1+\alpha+\alpha^2)\varepsilon:1]$	1101011100111111	p
17	$[\alpha^2+\alpha^2\varepsilon:1+\alpha^2+\alpha\varepsilon:1]$	0011001110110101	q
18	$[1+\alpha+\alpha^2+\alpha\varepsilon:\alpha+\alpha^2+\alpha\varepsilon:1]$	1111010101110101	r
19	$[\alpha+\alpha^2+\alpha\varepsilon:0:1]$	0111010100010001	s
20	$[1+\alpha^2+(1+\alpha^2)\varepsilon:\alpha+(\alpha+\alpha^2)\varepsilon:1]$	1011101101010111	t
21	$[\alpha^2\varepsilon:1+\varepsilon:1]$	0001001110011001	u
22	$[1+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:1+\alpha+\alpha^2+(1+\alpha)\varepsilon:1]$	1011111111111101	v
23	$[\alpha+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:\alpha+\alpha^2+\alpha^2\varepsilon:1]$	0111111101110011	w
24	$[1+\alpha\alpha^2+(1+\alpha)\varepsilon:1+(1+\alpha)\varepsilon:1]$	1111110110011101	x
25	$[\alpha^2+\alpha\varepsilon:1+(1+\alpha+\alpha^2)\varepsilon:1]$	0011010110011111	y
26	$[1+\alpha+\varepsilon:1+\alpha+\alpha^2+\alpha\varepsilon:1]$	1101100111110101	z
27	$[\alpha:\alpha^2+\alpha\varepsilon:1]$	0101000100110101	*space*
28	$[0:1:0]$	0000000010000000	.

5. Encryption and Decryption Technique

1) To encrypt the following message "use the elliptic curve" we follow these steps;
   a) remove the white space, the message becomes "usetheellipticcurve".
   b) choose a password for example "big".
   c) share the message in blocks of three letters, and w add g at the end of the message to balance "use/the/ell/ipt/icc/urv/egg"
   d) substitute the letters in each block with a cycle $(1, 2, 3)$, we get; " eus/eth/lel/tip/cic/vur/geg"
   e) build their codes according to the previouse table.

   • **Its encryption is:**
   011111110001110100010011100110010111010100010001
   011111110001110110111011010101111011101111111101
   110101111111100101111111000111011101011111111001
   101110110101011101110101011101011101011100111111
   110101110011111101110101011101011101011100111111
   101111111111110100010011100110011111010101110101
   000100111001101101111111000111010001001110011011

2) To decrypt the following message
   111101010111010101010001011101011101100111110101
   000100111001101101011101011110010001001110011011
   We follow these steps;
   a) gather the bits in the blocks of 48 bits.
   b) replace the blocks code on symbol letters.
   c) substitute the letters in each block with the reverse cycle.
   d) we get the resulte after completing the space and removing the g's wich are added.

   • **Its decryption is:** azro

Remark 5.1.
1) With this application, we can encrypt and decrypt any message of any lenth.This application can be implemented by Maple.
2) The motivation of this work is that decryption is difficult for an interceptor who doesn't know the password and a substitute cycle.

6. ACKNOWLEDGMENT

The first author is very very grateful to Faculty of science and Technical, Alhoceima, MOROCCO. The authors would like to thank Gulf Journal of Mathematics for its valued support.

References

[1] Abdelhamid Tadmori, Abdelhakim chillali and M'hamed Ziane; The Binary Operations Calculus in $E_{a,b,c}$; *International Journal of Mathematical Models and Methods in Applied Sciences*, Volume 9, 2015.

[2] Abdelhamid Tadmori, Abdelhakim chillali and M'hamed Ziane; Elliptic curves over ring $\mathbb{F}_{2^d}[\varepsilon]$; $\varepsilon^4 = 0$, *Applied Mathematical Sciences*, Vol. 9, 2015, no. 35, 1721 - 1733 HIKARI Ltd, www.m-hikari.com

[3] Abdelhamid Tadmori, Abdelhakim chillali and M'hamed Ziane; Elliptic Curves Over SPIR of characteristic Two; proceeding of the 2013 international conference on applied mathematics and Computational Methode,*www.europment.org/library/2013/AMCM-05.*

[4] Abdelhamid Tadmori, Abdelhakim chillali and M'hammed Ziane; Normal Form of the elliptic Curves over the finite ring; *Journal of Mathematics and system Sience* 4 (2014) 194-196.

[5] A. Joux and Vanessa Vitse, Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields Application to the static Diffie-Hellman problem on $\mathbf{E}(\mathbb{F}_{q^5})$. *Journal of cryptography*, volume 26 Issus 1, Jaunry Pages 119-143. Springer- Verlage New york.

[6] Igor Semaev, New algorithm for the discrete logarithm problem on elliptic curves. *Computer Science- and Security.* eprint.iacr.org/2015/310.

[7] J.H.SILVERMAN. The Arithmetic of Elliptic curves,*Graduate Texts in Mathematcs. Springer.*Volume 106(1985).2,19,20,21.

[8] J.H.SILVERMAN. Advanced Topics in the Arithmetic of Elliptic curves,*Graduate Texts in Mathematcs.* Volume 151, Springer,(1994).

[9] J. Lenstra, H.W, Elliptic curves and number-theoretic algorithms, *Processing of the International Congress of Mathematicians*,(Berkely,California,USA,1986).

[10] Mc Donald B. R., *Finite Rings with Identity, Inc. New York, Marcell Dekker, 1974.*

[11] M. VIRAT. Courbe elliptique sur un anneau et applications cryptographiques,*These Docteur en Sciences, Nice-Sophia Antipolis* (2009).

[12] N.KOBLITZ. Elliptic Curve Cryptosystems,*Mathematics of Computation.*48,203,209, (1987).2,6,21,37.

[13] R.LERCIER. Algorithmique de courbes elliptiques dans les corps finis,*PhD thesis, Ecole polytechnique.* juin (1997).

[14] V. Miller, Use of elliptic curves in cryptography, in CRYPTO'85, LNCS 218, pp.417-426, Springer 1986.

[15] W.Bosma and H.Lenstra,Complete system of two addition laws for elliptic curved, *Journal of Number theory* (1995).

[1] Department of Mathematics and Computer Sciences Faculty of Sceinces and technical, RDSI-Laboratory, Alhoceima, Abdelmalek Essaadi University, Morocco

Email address: [1] atadmori@yahoo.fr

[2] Department of Mathematics, Physics and Computing, LSI, FPT, University S.M. Ben Abdellah, Taza, Box 1223, Morocco

Email address: [2]abdelhakim.chillali@usmba.ac.ma

[3] Departement of Mathematics and Computer Sciences Faculty of Sceinces Oujda

Email address: [3]ziane12001@yahoo.fr