

Improved of Elliptic Curves Cryptography over a Ring

A. Chillali, A. Tadmori, M. Ziane

Abstract—In this article we will study the elliptic curve defined over the ring A_n and we define the mathematical operations of ECC, which provides a high security and advantage for wireless applications compared to other asymmetric key cryptosystem.

Keywords—Elliptic Curves, Finite Ring, Cryptography.

I. INTRODUCTION

THE ECC use curves whose variables coefficients are finite, there are two family commonly used on this cryptography. The first uses elliptic curves $E(\mathbb{F}_p)$ over prime finite field \mathbb{F}_p where p is large prime; this family is the best for software implementation of ECC. The second family use elliptic curves $E(\mathbb{F}_{2^d})$ over binary field \mathbb{F}_{2^d} where d is large integer number, this family is more suitable for hardware implementation of ECC. In this work, we define the other family which seems to be beneficial and interesting in ECC implementations. Its the family use elliptic curves $E_{a,b}(A_n)$ over the ring $A_n = \mathbb{F}_{2^d}[\epsilon]$ where $\epsilon^n = 0$, d and n are large integers numbers [1], [2], [7].

Let d be a positive integer, we consider the quotient ring $A_n = \frac{\mathbb{F}_{2^d}[X]}{(X^n)}$ where \mathbb{F}_{2^d} is the finite field of order 2^d . The ring A_n is identified to the ring $\mathbb{F}_{2^d}[\epsilon]; \epsilon^n = 0$. So, we have: $A_n = \{\sum_{i=0}^{n-1} x_i \epsilon^i | (x_i)_{0 \leq i \leq n-1} \in \mathbb{F}_{2^d}^n\}$. Similar as in [3] and in [5], we have the following lemmas:

Lemma 1. The elements non invertible in the ring A_n are the elements of ideal ϵA_n .

Proof: A_n is a local ring, its maximal ideal is $M = \epsilon A_n$.

Lemma 2. A_n is a vector space over \mathbb{F}_{2^d} of dimension n and $(1, \epsilon, \epsilon^2, \epsilon^3, \dots, \epsilon^{n-1})$ is a basis of A_n .

Lemma 3. Let $Y = \sum_{i=0}^{n-1} y_i \epsilon^i$ be the inverse of the element $X = \sum_{i=0}^{n-1} x_i \epsilon^i$ then:

$$\begin{cases} y_0 = x_0^{-1} \\ y_j = x_0^{-1} \cdot \sum_{i=0}^{j-1} y_i x_{j-i}. \text{ For } j = 1, 2, 3, \dots, n-1. \end{cases}$$

II. NOTATION

Definition 1. We define an elliptic curve over the ring A_n noted $E_{a,b}(A_n)$ as a curve given by such Weierstrass equation:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \quad (1)$$

where $a, b \in A_n$ that b is invertible.

A. Chillali is with the USMBA, LSI, FPT, Taza, Morocco (e-mail: abdelhakim.chillali@usmba.ac.ma).

A. Tadmori and M. Ziane were with UMP, FSO, Oujda, Morocco.

The discriminant $\Delta = b$ and the J-invariant $J = \frac{1}{b}$, we write:

$$E_{a,b}(A_n) = \{[X:Y:Z] \in \mathbb{P}_2(A_n) | Y^2Z + XYZ = X^3 + aX^2Z + bZ^3\}$$

Definition 2. We define a reduction of $E_{a,b}(A_n)$ over \mathbb{F}_{2^d} as a curve given by such Weierstrass equation:

$$Y^2Z + XYZ = X^3 + a_0X^2Z + b_0Z^3 \quad (2)$$

where $a_0, b_0 \in \mathbb{F}_{2^d}$ that $b_0 \neq 0$.

The discriminant $\Delta_0 = b_0$ and the j-invariant $j = \frac{1}{b_0}$, we write:

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

Notation 1. We denote π the canonical projection by:

$$\pi: A_n \rightarrow \mathbb{F}_{2^d} \\ \sum_{i=0}^{n-1} x_i \epsilon^i \mapsto x_0$$

III. CLASSIFICATION OF ELEMENTS OF $E_{a,b}(A_2)$

Let $[X:Y:Z] \in E_{a,b}(A_2)$, where X, Y and Z are in A . 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 $Z = z_1\epsilon$, see [4], in this cases we have tow cases for Y .

- Y Invertible:

Then $[X:Y:Z] = [XY^{-1}:1:ZY^{-1}]$; so we just take $[X:1:z_1\epsilon]$; then is verified the equation of

$$E_{a,b}(A): Y^2Z + XYZ = X^3 + aX^2Z + bZ^3,$$

so we can write:

$$\begin{aligned} a &= a_0 + a_1\epsilon \\ b &= b_0 + b_1\epsilon \\ X &= x_0 + x_1\epsilon \end{aligned}$$

We have:

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

which implies that

$$z_1\epsilon + x_0z_1\epsilon = x_0^3 + (x_0^2x_1 + a_0x_0^2z_1)\epsilon$$

Then

$$(z_1 + x_0z_1)\epsilon = x_0^3 + (x_0^2x_1 + a_0x_0^2z_1)\epsilon$$

- Y Non Invertible:

Proposition 1. Every element of $E_{a,b}(A)$, is of the form $[X:Y:1]$ or $[x\varepsilon:1:0]$, where $x \in F_{2^d}$ and we write:

Theorem 1. Let $P = [X_1:Y_1:Z_1], Q = [X_2:Y_2:Z_2]$ in $E_{a,b}(A)$ then $P + Q = [X_3:Y_3:Z_3]$:

- $$\begin{aligned} X_3 &= X_1 Y_1 Y_2 + X_2 Y_1^2 Y_2 + X_2^2 Y_1^2 + X_1 X_2^2 Y_1 + a X_1^2 X_2 Y_2 \\ &\quad + a X_1 X_2^2 Y_1 + a X_1^2 X_2^2 + b X_1 Y_1 Z_2^2 \\ &\quad + b X_2 Y_2 Z_1^2 + b X_1^2 Z_2^2 + b Y_1 Z_2^2 Z_1 \\ &\quad + b Y_2 Z_1^2 Z_2 + b X_1 Z_2^2 Z_1 \\ Y_3 &= Y_1^2 Y_2^2 + X_2 Y_1^2 Y_2 + a X_1 X_2^2 Y_1 + a^2 X_1^2 X_2^2 + b X_1^2 X_2 Z_2 \\ &\quad + b X_1 X_2^2 Z_1 + b X_1 Y_1 Z_2^2 + b X_1^2 Z_2^2 \\ &\quad + ab X_2^2 Z_1^2 + b Y_1 Z_2^2 Z_1 + b X_1 Z_2^2 Z_1 \\ &\quad + ab X_1 Z_2^2 Z_1 + ab X_2 Z_1^2 Z_2 + b^2 Z_1^2 Z_2^2 \\ Z_3 &= X_1^2 X_2 Y_2 + X_1 X_2^2 Y_1 + Y_1^2 Y_2 Z_2 + Y_1 Y_2^2 Z_1 + X_1^2 X_2^2 \\ &\quad + X_2 Y_1^2 Z_2 + X_1^2 Y_2 Z_2 + a X_1^2 Y_2 Z_2 + a X_2^2 Y_1 Z_1 \\ &\quad + X_1^2 X_2 Z_2 + a X_1 X_2^2 Z_1 + b Y_1 Z_2^2 Z_1 \\ &\quad + b Y_2 Z_1^2 Z_2 + b X_1 Z_2^2 Z_1 \end{aligned}$$

- $$\begin{aligned} X_3 &= X_1 Y_2^2 Z_1 + X_2 Y_1^2 Z_2 + X_1^2 Y_2 Z_2 + X_2^2 Y_1 Z_1 + a X_1^2 X_2 Z_2 \\ &\quad + a X_1 X_2^2 Z_1 + b X_1 Z_2^2 Z_1 + b X_2 Z_1^2 Z_2 \\ Y_3 &= X_1^2 X_2 Y_2 + X_1 X_2^2 Y_1 + Y_1^2 Y_2 Z_2 + Y_1 Y_2^2 Z_1 + X_1^2 Y_2 Z_2 \\ &\quad + X_2^2 Y_1 Z_1 + a X_1^2 Y_2 Z_2 + a X_2^2 Y_1 Z_1 \\ &\quad + a X_1^2 X_2 Z_2 + a X_1 X_2^2 Z_1 + b Y_1 Z_2^2 Z_1 \\ &\quad + b Y_2 Z_1^2 Z_2 + b X_1 Z_2^2 Z_1 + b X_2 Z_1^2 Z_2 \\ Z_3 &= X_1^2 X_2 Z_2 + X_1 X_2^2 Z_1 + Y_1^2 Z_2^2 + Y_2^2 Z_1^2 + X_1 Y_1 Z_2^2 \\ &\quad + X_2 Y_2 Z_1^2 + a X_1^2 Z_2^2 + a X_2^2 Z_1^2 \end{aligned}$$

IV. CRYPTOGRAPHY APPLICATION

- Coding of Elements of G .

Let $Q = [\sum_{i=0}^{n-1} x_i \varepsilon^i : \sum_{i=0}^{n-1} y_i \varepsilon^i : Z]$ where, $x_i, y_i \in \mathbb{F}_{2^d}$, for $i = 0, 1, \dots, n-1$ and $Z = \sum_{i=3}^{n-1} z_i \varepsilon^i$, or $Z = 1$.

$$x_i = c_{0,i} + c_{1,i}\alpha + \dots c_{(d-1),i}\alpha^{d-1} = c_{0,i}c_{1,i} \dots c_{(d-1),i}$$
$$Q = \underbrace{x_0x_1 \dots x_{n-1}y_0y_1 \dots y_{n-1}}_{3.d.n}10 \dots 0$$

- $$Q = \underbrace{0 \dots 0x_1 \dots x_{n-1} 10 \dots 0z_3 \dots z_{n-1}}_{3.d.n}$$

- Remark 1.** With the secret key S' such as the decimal code of point **S** Alice and Bob can encrypt and decrypt the message (m) .

-
- ```

graph TD
 M[Message m] --> DTD[Determine a, b, d, P]
 DTD --> SSC[Select suitable curve and G<P>]
 SSC --> EKE[Echange of key]
 EKE --> A[Alice chooses t and compute tP]
 EKE --> B[Bob chooses l and compute lP]
 A -- sends --> C[Calculates S=t.lP]
 B -- sends --> D[Calculates S=l.tP]
 C --> SK[Choose the decimal code of the point S as secret keys']
 D --> SK
 SK --> ENC[Encode the message m on point Pm]
 ENC --> CM[Choose randomly k]
 CM --> QK[Calculate Q=kPm]
 QK -- Send Q --> PK[Calculate Pbkey=S'Q]
 PK --> PK1[Public key is a, b, d, P, Pbkey, Q]
 PK --> PK2[Private key is t, l, k, s']
 PK1 --> PK2
 PK2 --> PK1

```
- The flowchart illustrates the Diffie-Hellman key exchange process. It begins with a message  $m$ , which is used to determine parameters  $a, b, d, P$ . A suitable curve and group  $G \langle P \rangle$  are selected. The process then enters an 'Echange of key' phase where Alice chooses  $t$  and computes  $tP$ , while Bob chooses  $l$  and computes  $lP$ . They exchange these values. Alice then calculates  $S = t.lP$  and Bob calculates  $S = l.tP$ . Both calculate the same point  $S$ , which is then converted to a decimal code to serve as a secret key. This key is used to encode the message  $m$  on point  $P_m$ . A random value  $k$  is chosen to calculate  $Q = kP_m$ . This value  $Q$  is sent to the other party, who then calculates the public key  $P_{bkey} = S'Q$ . The final output consists of the public key  $(a, b, d, P, P_{bkey}, Q)$  and the private key  $(t, l, k, s')$ .

Fig. 1 Depict the key generation phase

$$(P_m + r.Pbkey) - S'.(r.Q) = P_m + r.S'.Q - S'.r.Q = P_m$$

This operation is shown in Fig. 3.

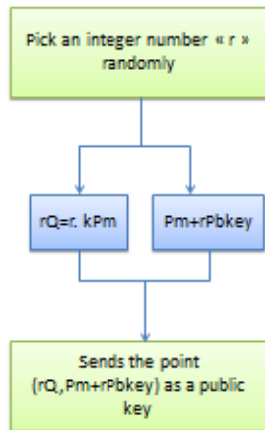


Fig. 2 The encryption operation

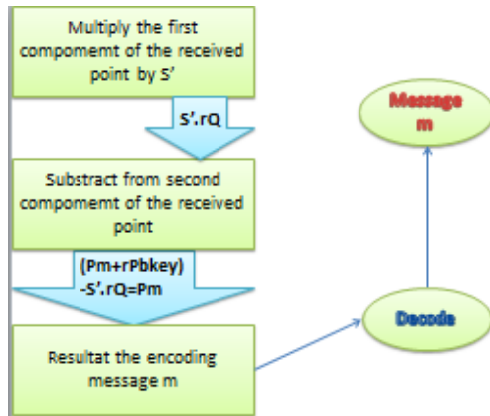


Fig. 3 Decrypting the message

#### • Example.

For the example we take the case  $n = 3$  (i.e.:  $E_{a,b}(A_3)$ ) and let  $\alpha$  is a primitive root of an irreducible polynomial  $R(X) = X^3 + X + 1$  over  $\mathbb{F}_2$ .

We consider the field  $\mathbb{F}_2(\alpha) = \frac{\mathbb{F}_2[X]}{(R(X))} \cong \mathbb{F}_8$ ,  $\mathbb{F}_8$  is the finite field of order  $2^3$  and of basis  $(1, \alpha, \alpha^2)$ .

Let  $a = 1 + \alpha + \alpha\epsilon + \epsilon^2$ ,  $b = 1 + \alpha^2\epsilon + \epsilon^2$  two elements of  $A_3$ .

The elliptic curve  $E_{a,b}(A_3)$  has 896 elements but the elliptic curve  $E_{a_0,b_0}(\mathbb{F}_8)$ , where  $a_0 = \pi(a)$ , and  $b_0 = \pi(b)$  has 14 elements.

So, we have well:  $\#E_{a,b}(A_3) = \#E_{a_0,b_0}(\mathbb{F}_8) \times \#\mathbb{F}_8^2$ .

We consider the point  $P = [\alpha^2 + \alpha^2\epsilon + \alpha\epsilon^2: 1 + \alpha^2 + \epsilon: 1]$ , we have  $G = \langle P \rangle$  is the subgroup of order 56 so, for  $Q \in G, \exists m \in \{1, 2, \dots, 56\}: Q = mP$ .

The points of  $G$  are:

$$\begin{aligned}
 P &= [\alpha^2 + \alpha^2\epsilon + \alpha\epsilon^2: 1 + \alpha^2 + \epsilon: 1] \\
 2P &= [1 + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha + (\alpha^2 + 1)\epsilon + \epsilon^2: 1] \\
 3P &= [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha + \alpha^2 + (\alpha + 1) + \alpha^2\epsilon^2: 1] \\
 4P &= [1 + \alpha + (\alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 5P &= [\alpha + (\alpha + \alpha^2)\epsilon^2: \alpha + \alpha^2 + (\alpha + \alpha^2)\epsilon: 1] \\
 6P &= [1 + \alpha + \alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon: 1] \\
 7P &= [\alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1 + (1 + \alpha^2)\epsilon + \epsilon^2: 1] \\
 8P &= [1 + \alpha + \alpha^2 + (1 + \alpha)\epsilon + (1 + \alpha)\epsilon^2: 1 + (\alpha + \alpha^2)\epsilon + \alpha\epsilon^2: 1]
 \end{aligned}$$

$$\begin{aligned}
 9P &= [\alpha + (1 + \alpha)\epsilon + (1 + \alpha)\epsilon^2: \alpha^2 + (\alpha^2 + \alpha)\epsilon + \alpha^2\epsilon^2: 1] \\
 10P &= [1 + \alpha + \epsilon + (1 + \alpha + \alpha^2)\epsilon^2: \alpha^2 + (1 + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 11P &= [\alpha + \alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: (1 + \alpha + \alpha^2)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 12P &= [1 + \alpha^2 + (1 + \alpha^2)\epsilon + \epsilon^2: 1 + \alpha + \alpha^2 + \alpha\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 13P &= [\alpha^2 + \alpha\epsilon + \epsilon^2: 1 + \alpha^2\epsilon + \epsilon^2: 1] \\
 14P &= [\alpha^2\epsilon + \epsilon^2: 1: 0] \\
 15P &= [\alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: 1 + \alpha^2 + (\alpha^2 + \alpha)\epsilon + \epsilon^2: 1] \\
 16P &= [1 + \alpha^2 + (1 + \alpha^2)\epsilon + \alpha\epsilon^2: \alpha + (1 + \alpha + \alpha^2) + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 17P &= [\alpha + \alpha^2 + \alpha\epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 18P &= [1 + \alpha + \epsilon + (\alpha + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + \alpha^2\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 19P &= [\alpha + (1 + \alpha)\epsilon + \alpha^2\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2)\epsilon: 1] \\
 20P &= [1 + \alpha + \alpha^2 + (1 + \alpha)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2)\epsilon + \alpha\epsilon^2: 1] \\
 21P &= [\alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1 + \epsilon + \alpha\epsilon^2: 1] \\
 22P &= [1 + \alpha + \alpha^2 + \alpha\epsilon: 1 + (1 + \alpha^2)\epsilon + (1 + \alpha)\epsilon^2: 1] \\
 23P &= [\alpha + \epsilon^2: \alpha^2 + (\alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 24P &= [1 + \alpha + (\alpha + \alpha^2)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: \alpha^2 + \epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 25P &= [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + \alpha^2\epsilon^2: \alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 26P &= [1 + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (1 + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + \alpha\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 27P &= [\alpha^2 + \alpha^2\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1 + (1 + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 28P &= [(\alpha + \alpha^2)\epsilon^2: 1: 0] \\
 29P &= [\alpha^2 + \alpha^2\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1 + \alpha^2 + \epsilon + \epsilon^2: 1] \\
 30P &= [1 + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (1 + \alpha^2)\epsilon^2: \alpha + (1 + \alpha^2)\epsilon + \alpha\epsilon^2: 1] \\
 31P &= [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + \alpha^2\epsilon^2: \alpha + \alpha^2 + (1 + \alpha)\epsilon + \epsilon^2: 1] \\
 32P &= [1 + \alpha + (\alpha + \alpha^2)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + \alpha\epsilon^2: 1] \\
 33P &= [\alpha + \epsilon^2: \alpha + \alpha^2 + (\alpha + \alpha^2)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 34P &= [1 + \alpha + \alpha^2 + \alpha\epsilon: \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (1 + \alpha)\epsilon^2: 1] \\
 35P &= [\alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1 + (1 + \alpha^2)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 36P &= [1 + \alpha + \alpha^2 + (1 + \alpha)\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1 + (\alpha + \alpha^2)\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 37P &= [\alpha + (1 + \alpha)\epsilon + \alpha^2\epsilon^2: \alpha^2 + (\alpha + \alpha^2)\epsilon + \alpha^2\epsilon^2: 1] \\
 38P &= [1 + \alpha + \epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha^2 + (1 + \alpha^2)\epsilon: 1] \\
 39P &= [\alpha + \alpha^2 + \alpha + (\alpha + \alpha^2)\epsilon^2: (1 + \alpha + \alpha^2)\epsilon: 1] \\
 40P &= [1 + \alpha^2 + (1 + \alpha^2)\epsilon + \alpha\epsilon^2: 1 + \alpha + \alpha^2 + \alpha\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 41P &= [\alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: 1 + \alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1] \\
 42P &= [\alpha^2\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1: 0] \\
 43P &= [\alpha^2 + \alpha\epsilon + \epsilon^2: 1 + \alpha^2 + (\alpha + \alpha^2)\epsilon: 1] \\
 44P &= [1 + \alpha^2 + (1 + \alpha^2)\epsilon + \epsilon^2: \alpha + (1 + \alpha + \alpha^2)\epsilon + \alpha^2\epsilon^2: 1] \\
 45P &= [\alpha + \alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2)\epsilon + (1 + \alpha)\epsilon^2: 1] \\
 46P &= [1 + \alpha + \epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + \alpha^2\epsilon + \epsilon^2: 1] \\
 47P &= [\alpha + (1 + \alpha)\epsilon + (1 + \alpha)\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2) + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 48P &= [1 + \alpha + \alpha^2 + (1 + \alpha)\epsilon + (1 + \alpha)\epsilon^2: \alpha + \alpha^2 + (1 + \alpha^2)\epsilon + \epsilon^2: 1] \\
 49P &= [\alpha^2\epsilon + (1 + \alpha^2)\epsilon^2: 1 + \epsilon + \alpha^2\epsilon^2: 1] \\
 50P &= [1 + \alpha + \alpha^2 + \alpha\epsilon + \alpha^2\epsilon^2: 1 + (1 + \alpha^2)\epsilon + \alpha^2\epsilon^2: 1] \\
 51P &= [\alpha + (\alpha + \alpha^2)\epsilon^2: \alpha^2 + (\alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1] \\
 52P &= [1 + \alpha + (\alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha^2 + \epsilon + (1 + \alpha)\epsilon^2: 1] \\
 53P &= [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: \alpha^2\epsilon + \alpha\epsilon^2: 1] \\
 54P &= [1 + \alpha^2 + (1 + \alpha + \alpha^2)\epsilon + (\alpha + \alpha^2)\epsilon^2: 1 + \alpha + \alpha^2 + \alpha\epsilon + (1 + \alpha + \alpha^2)\epsilon^2: 1] \\
 55P &= [\alpha^2 + \alpha^2\epsilon + \alpha\epsilon^2: 1 + (1 + \alpha^2)\epsilon + \alpha\epsilon^2: 1] \\
 56P &= [0: 1: 0]
 \end{aligned}$$

• Table of Coding the Elements of  $\mathbb{G}$

We use English letters for this application. The coding are as follows:

TABLE I  
TABLE OF LETTERS

| Code of m.P                | Symbol |
|----------------------------|--------|
| 00100101010110000010000000 | a      |
| 10111101101010110010000000 | b      |
| 01111101101110001100000000 | c      |
| 11001101111111011000000000 | d      |
| 01000001101101100010000000 | e      |
| 11101000101111100010000000 | f      |
| 00000110110010110010000000 | g      |
| 11111011010001101010000000 | h      |
| 01011011000101100110000000 | i      |
| 11010011001101011100000000 | j      |
| 01101000100011111110000000 | k      |
| 10110110011101010110000000 | l      |
| 00101010010000110010000000 | m      |
| 00000110010000000000000000 | n      |
| 00101000110101110010000000 | o      |
| 10110101001011111110000000 | p      |
| 01101001101110101110000000 | q      |
| 11010001111100101110000000 | r      |
| 01011000101110100010000000 | s      |
| 11111011101110101010000000 | t      |
| 00000110110010001010000000 | u      |
| 11101000100101110100000000 | v      |
| 01000010000101101110000000 | w      |
| 11001111001100101100000000 | x      |
| 01111100100000110110000000 | y      |
| 10111101111010111100000000 | z      |
| 00100111100101011100000000 | (      |
| 00000001110000000000000000 | )      |
| 00100111101100100100000000 | ;      |
| 10111101010101010100000000 | !      |
| 01111100101111010010000000 | :      |
| 11001111111111010100000000 | \$     |
| 01000010001101111100000000 | .      |
| 11101000001111110100000000 | @      |
| 00000110110010111110000000 | >      |
| 11111011100011011000000000 | <      |
| 01011000100101100110000000 | %      |
| 11010001100110100010000000 | £      |
| 01101001100011100010000000 | \$     |
| 10110101011101010110000000 | /      |
| 00101000110000110110000000 | ?      |
| 00000111110000000000000000 |        |
| 00101010010110001000000000 | #      |
| 10110110001011100110000000 | 0      |
| 01101000101110111010000000 | 1      |
| 11010011111100110010000000 | 2      |
| 01011010011101111000000000 | 3      |
| 11111011001110110010000000 | 4      |
| 00000110110010001100000000 | 5      |
| 11101000110010100110000000 | 6      |
| 01000001100101101110000000 | 7      |
| 11001101100110011010000000 | 8      |
| 01111101100000101010000000 | 9      |
| 10111101111010111100000000 | ,      |
| 00100101010010101010000000 | space  |
| 00000000100000000000000000 | ~      |

• Encryption and Decryption Messages

Let the following message: "nlmad tamazivt"

Transmutation this message effected letter by letter, its points codes are:

TABLE II  
TABLE OF ENCRYPT

| Code of letters            | Symbol |
|----------------------------|--------|
| 00100101010110000010000000 | a      |
| 11001101111111110110000000 | d      |
| 00101010010000110010000000 | m      |
| 00000110010000000000000000 | n      |
| 11111011101110101010000000 | t      |
| 00000110110010001010000000 | u      |
| 11101000100101110100000000 | v      |
| 10111101111010111100000000 | z      |
| 10110110011101010110000000 | l      |
| 01011011000101100110000000 | i      |

The encryption and decryption of these points are effected by the process cited before see, Figs. 1 and 2.

Exchange of Secret Key.

Alice chooses a random number  $t = 5$  and computes  $K = t.P$ .

Alice sends  $K$  to Bob, but keep  $t$ .

Bob chooses a random number  $= 7$ , computes  $K' = l.P$ .

Bob sends  $K'$  to Alice, but keep  $l$ .

Alice computes  $tK' = 35P$ .

Bob computes  $lK = 35P$ .

Alice and Bob are agree with a point  $S = 35P$ , choose the code of point  $S$  as a private key, which transformed on the decimal code  $S' = 3563264$

To encrypt every point  $P_m$ , a user picks an integer «  $r$  » at random and sends the point  $(r.Q, P_m + r.Pbkey)$ .

We have the following text:

(10111101101010110010000000,01111101101111000110000000)(11001101111111110110000000,01000001101101100100000000)(11101000101111000100000000,000001101100101100100000000)(11111011010001101010000000,010110110001011001100000000)(11010011100110101110000000,0,01101000100011111100000000)(1011011100111010110000000,001010100100001100100000000)(000001100100000000000000,001010001101011100100000000)(1011101101010110010000000,01111101101111000110000000)(11001101111111110110000000,01000001101101100100000000)(11101000101111100010000000,000001101100101100100000000)(11111011010001101010000000,010110110001011001100000000)(11010011100110101110000000,0,01101000100011111100000000)(101101100111010110000000,001010100100001100100000000)(000001100100000000000000,001010001101011100100000000)

**Remark 2.** With this application, we can encrypt and decrypt any message. The security of this encryption is based on the discrete logarithm problem.

V.CONCLUSION

In this work, we have studied the elliptic curves cryptography over the ring  $A_n = \mathbb{F}_{2^d}[\varepsilon]$ ;  $\varepsilon^n = 0$ , and we have established the coding over the elliptic curves  $E_{a,b}(A_n)$ .

Further, the Discrete Logarithm Problem (DLP) on this elliptic curve is equivalent to the one on  $E_{a_0,b_0}(\mathbb{F}_{2^d})$  but the cardinal of this elliptic curve is bigger than that of  $E_{a_0,b_0}(\mathbb{F}_{2^d})$ , which seems to be beneficial and interesting in cryptography.

#### ACKNOWLEDGMENT

The authors would like to thank University of Mohammed First Oujda and USMBA, FSI, FPT of Taza in MOROCCO for its valued support.

#### REFERENCES

- [1] A. Chillali, The  $j$ -invariant over  $E_{3^d}^n$ , Int.j.Open problems Compt. Math.Vol.5, No 4,December 2012,ISSN 1998-6262, Copyright ICSRS Publication, (WWW.i-csrs.org,pp.106-111, 2012).
- [2] A. Chillali, Cryptography over elliptic curve of the ring  $\mathbb{F}_q[\epsilon]$ ,  $\epsilon^4 = 0$  World Academy of science Engineering and Technology, 78 (2011), pp.848-850
- [3] A. Chillali, Elliptic curve over ring, International Mathematical Forum, Vol.6, no.31, 2011 pp.1501-1505
- [4] A. Tadmori, A. Chillali and M. 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](http://www.europment.org/library/2013/AMCM-05).
- [5] A. Tadmori, A. Chillali and M. Ziane, Normal Form of the elliptic Curves over the finite ring, Journal of Mathematics and system Sience, 4 (2014) 194-196.
- [6] A. Tadmori, A. Chillali and M. Ziane, Coding over elliptic curves in the ring of characteristic two, International journal of Applied Mathematics and Informatics, (Volume 8. 2014).
- [7] A. Tadmori, A. Chillali and M. Ziane, The binary operations calculus in  $E_{a,b,c}$ , International Journal of Mathematical Models and Methods in Applied Sciences, Volume 9, p:171-175,( 2015 ).
- [8] W. Bosma and H. Lenstra, Complete system of two addition laws for elliptic curved, Journal of Number theory, (1995).