International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:9, No:4, 2015

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 An 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 benefical and interesting in ECC implementations. Its the family use elliptic curves $E_{a,b}(A_n)$ over the ring $A_n = \mathbb{F}_{2^d}[\varepsilon]$ where $\varepsilon^n = 0$, 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 $\mathbb{F}_{2^d}[\varepsilon]; \varepsilon^n = 0$. So, we have: $A_n = \{\sum_{i=0}^{n-1} x_i \varepsilon^i | (x_i)_{0\le i\le n-1} \in \mathbb{F}^n{}_{2^d}\}$. 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 $M = \varepsilon A_n$.

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

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

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

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:

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

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

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:

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

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:

$$\pi: A_n \longrightarrow \mathbb{F}_{2^d}$$
$$\sum_{i=0}^{n-1} x_i \varepsilon^i \longmapsto x_0$$

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 $Z = z_1\varepsilon$, 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 : $z_1\varepsilon$]; then is verified the equation of

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

so we can write:

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

We have:

$$z_1\varepsilon + (x_0 + x_1\varepsilon).z_1 = (x_0 + x_1\varepsilon)^3 + (a_0 + a_1\varepsilon).(x_0 + x_1\varepsilon)^2.z_1\varepsilon + (b_0 + b_1\varepsilon).z_1{}^3\varepsilon^3$$

which implies that

$$z_1\varepsilon + x_0z_1\varepsilon = x_0{}^3 + (x_0{}^2x_1 + a_0x_0{}^2z_1)\varepsilon$$

Then

$$(z_1 + x_0z_1)\varepsilon = x_0{}^3 + (x_0{}^2x_1 + a_0x_0{}^2z_1)\varepsilon$$

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.

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

- Y Non Invertible:

Then we have $Y = y_1\varepsilon$, so$X = x_0 + x_1\varepsilon$ is invertible so 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 1. Every element of $E_{a,b}(A)$, is of the form $[X:Y:1]$ or $[x\varepsilon:1:0]$, where $x \in \mathbb{F}_{2^d}$ and we write:

$$E_{a,b}(A) = \{[X:Y:1] \in P_2(A) | Y^2 + XY = X^3 + aX^2 + b\} \cup \{[x\varepsilon:1:0] | x \in \mathbb{F}_{2^d}\}. [1, 4].$$

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

- If $\pi_2(P) = \pi_2(Q)$ then:

$$\begin{aligned}
X_3 = {} & X_1Y_1Y_2 + X_2{Y_1}^2Y_2 + {X_2}^2{Y_1}^2 + X_1{X_2}^2Y_1 + a\,{X_1}^2X_2Y_2 \\
& + a\,X_1{X_2}^2Y_1 + a\,{X_1}^2{X_2}^2 + b\,X_1Y_1{Z_2}^2 \\
& + b\,X_2Y_2{Z_1}^2 + b\,{X_1}^2{Z_2}^2 + b\,Y_1{Z_2}^2Z_1 \\
& + b\,Y_2{Z_1}^2Z_2 + b\,X_1{Z_2}^2Z_1 \\
Y_3 = {} & {Y_1}^2{Y_2}^2 + X_2{Y_1}^2Y_2 + a\,X_1{X_2}^2Y_1 + a^2{X_1}^2{X_2}^2 + b\,{X_1}^2X_2Z_2 \\
& + b\,X_1\,{X_2}^2Z_1 + b\,X_1Y_1{Z_2}^2 + b\,{X_1}^2{Z_2}^2 \\
& + ab\,{X_2}^2{Z_1}^2 + b\,Y_1{Z_2}^2Z_1 + b\,X_1{Z_2}^2Z_1 \\
& + ab\,X_1{Z_2}^2Z_1 + ab\,X_2{Z_1}^2Z_2 + b^2{Z_1}^2{Z_2}^2 \\
Z_3 = {} & {X_1}^2X_2Y_2 + X_1{X_2}^2Y_1 + {Y_1}^2Y_2Z_2 + Y_1{Y_2}^2Z_1 + {X_1}^2{X_2}^2 \\
& + X_2{Y_1}^2Z_2 + {X_1}^2Y_2Z_2 + a\,{X_1}^2Y_2Z_2 + a\,{X_2}^2Y_1Z_1 \\
& + {X_1}^2X_2Z_2 + a\,X_1{X_2}^2Z_1 + b\,Y_1{Z_2}^2Z_1 \\
& + b\,Y_2{Z_1}^2Z_2 + b\,X_1{Z_2}^2Z_1
\end{aligned}$$

- If $\pi_2(P) \neq \pi_2(Q)$ then:

$$\begin{aligned}
X_3 = {} & X_1{Y_2}^2Z_1 + X_2{Y_1}^2Z_2 + {X_1}^2Y_2Z_2 + {X_2}^2Y_1Z_1 + a\,{X_1}^2X_2Z_2 \\
& + a\,X_1{X_2}^2Z_1 + b\,X_1{Z_2}^2Z_1 + b\,X_2{Z_1}^2Z_2 \\
Y_3 = {} & {X_1}^2X_2Y_2 + X_1{X_2}^2Y_1 + {Y_1}^2Y_2Z_2 + Y_1{Y_2}^2Z_1 + {X_1}^2Y_2Z_2 \\
& + {X_2}^2Y_1Z_1 + a\,{X_1}^2Y_2Z_2 + a\,{X_2}^2Y_1Z_1 \\
& + a\,{X_1}^2X_2Z_2 + a\,X_1X_2{Z_1}^2 + b\,Y_1{Z_2}^2Z_1 \\
& + b\,Y_2{Z_1}^2Z_2 + b\,X_1{Z_2}^2Z_1 + b\,X_2{Z_1}^2Z_2 \\
Z_3 = {} & {X_1}^2X_2Z_2 + X_1{X_2}^2Z_1 + {Y_1}^2{Z_2}^2 + {Y_2}^2{Z_1}^2 + X_1Y_1{Z_2}^2 \\
& + X_2Y_2{Z_1}^2 + a\,{X_1}^2{Z_2}^2 + a\,{X_2}^2{Z_1}^2
\end{aligned}$$

Proof: Using the explicit formulas in [8] we prove the theorem.

IV. Cryptography Application

Let $P \in E_{a,b}(A_n)$ of order ρ, we will use the subgroup $< P >$ of $E_{a,b}(A_n)$ to encrypt message, and we denote $G =< P >$.

- Coding of Elements of G.

We will give a code to each element $Q = m.P \in G$, where $m \in \{1, 2, \ldots \rho\}$.

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 $i = 0, 1, \ldots, n-1$ and $Z = \sum_{i=3}^{n-1} z_i\,\varepsilon^i$, or $Z = 1$.

We set:

$$x_i = c_{0,i} + c_{1,i}\alpha + \cdots c_{(d-1),i}\alpha^{d-1} = c_{0,i}c_{1,i} \ldots c_{(d-1),i}$$

where α is a primitive root of an irreducible polynomial of degree d over $\mathbb{F}_2$ then, we code Q as it follows:[6]

- If $Q = [\sum_{i=0}^{n-1} x_i\,\varepsilon^i : \sum_{i=0}^{n-1} y_i\,\varepsilon^i : 1]$, then:

$$Q = \underbrace{x_0x_1 \ldots x_{n-1}y_0y_1 \ldots y_{n-1}10 \ldots 0}_{3.d.n}$$

- If $Q = [\sum_{i=1}^{n-1} x_i\,\varepsilon^i : 1 : \sum_{i=3}^{n-1} z_i\,\varepsilon^i]$, then:

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

- Exchange of Secret Key

Alice and Bob wants exchange the secret key, for this he start publicly with integer d, a curve elliptic $E_{a,b}(A_n)$, a point $P \in E_{a,b}(A_n)$ of order ρ and the coding methode over $G =< P >$.

Alice chooses a random number $0 \leq t \leq \rho - 1$ and computes $K = tP$.

Alice sends K to Bob, but keep t

Bob chooses a random number $0 \leq l \leq \rho - 1$, computes $K' = lP$.

Bob sends K' to Alice, but keep l.

Alice computes $t.K' = t.lP$.

Bob computes $l.K = l.tP$.

Finally, Alice and Bob are agree with a point $S = t.lP$, choose the binary code of point S as a private key, which transformed on the decimal code « S′ ».

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).

- ECC Key Generation Block Diagram

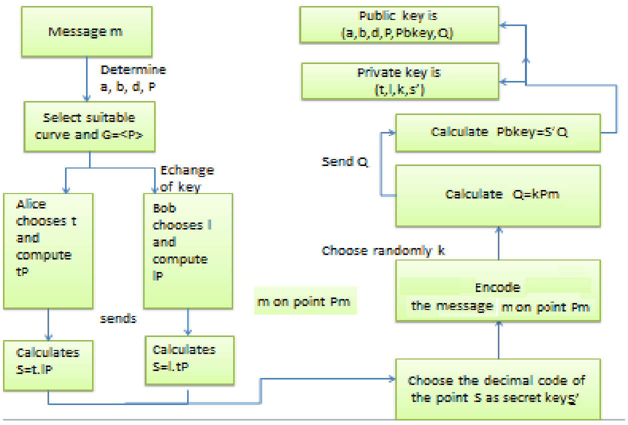

Fig. 1 Depict the key generation phase

To encrypt P_m, a user picks an integer « r » at random and sends the point $(r.Q, P_m + r.Pbkey)$. This operation is showed in Fig. 2.

- ECC Encryption Process Block Diagram

Decryption this message is done by multiplying the first component of the received point by the secret key « S′ » and substract it from the second component:

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

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:9, No:4, 2015

This operation is shown in Fig. 3.

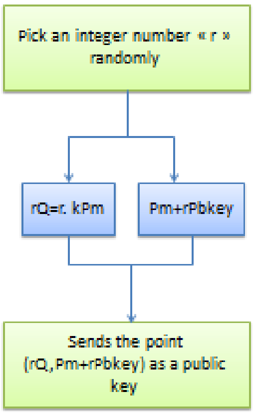

Fig. 2 The encryption operation

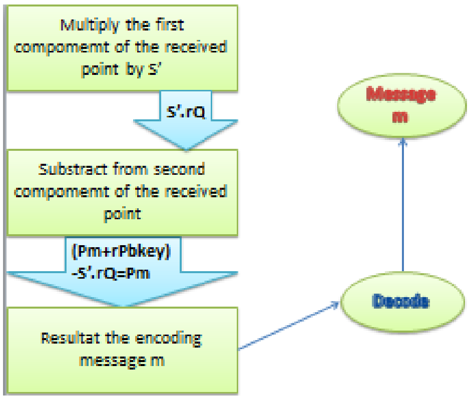

Fig. 3 Decrypting the message

- Example.

For the example we take the case $n = 3$ (i.e.: $E_{a,b}(A_3)$) and let α 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 $a = 1 + \alpha + \alpha\varepsilon + \varepsilon^2, b = 1 + \alpha^2\varepsilon + \varepsilon^2$ 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 $P = [\alpha^2 + \alpha^2\varepsilon + \alpha\varepsilon^2 : 1 + \alpha^2 + \varepsilon : 1]$, we have $G =< P >$ 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:

$P = [\alpha^2 + \alpha^2\varepsilon + \alpha\varepsilon^2 : 1 + \alpha^2 + \varepsilon : 1]$
$2P = [1 + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha + (\alpha^2 + 1)\varepsilon + \varepsilon^2 : 1]$
$3P = [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha + \alpha^2 + (\alpha + 1) + \alpha^2\varepsilon^2 : 1]$
$4P = [1 + \alpha + (\alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$5P = [\alpha + (\alpha + \alpha^2)\varepsilon^2 : \alpha + \alpha^2 + (\alpha + \alpha^2)\varepsilon : 1]$
$6P = [1 + \alpha + \alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon : 1]$
$7P = [\alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1 + (1 + \alpha^2)\varepsilon + \varepsilon^2 : 1]$
$8P = [1 + \alpha + \alpha^2 + (1 + \alpha)\varepsilon + (1 + \alpha)\varepsilon^2 : 1 + (\alpha + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1]$
$9P = [\alpha + (1 + \alpha)\varepsilon + (1 + \alpha)\varepsilon^2 : \alpha^2 + (\alpha^2 + \alpha)\varepsilon + \alpha^2\varepsilon^2 : 1]$
$10P = [1 + \alpha + \varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : \alpha^2 + (1 + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$11P = [\alpha + \alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : (1 + \alpha + \alpha^2)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$12P = [1 + \alpha^2 + (1 + \alpha^2)\varepsilon + \varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$13P = [\alpha^2 + \alpha\varepsilon + \varepsilon^2 : 1 + \alpha^2\varepsilon + \varepsilon^2 : 1]$
$14P = [\alpha^2\varepsilon + \varepsilon^2 : 1 : 0]$
$15P = [\alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : 1 + \alpha^2 + (\alpha^2 + \alpha)\varepsilon + \varepsilon^2 : 1]$
$16P = [1 + \alpha^2 + (1 + \alpha^2)\varepsilon + \alpha\varepsilon^2 : \alpha + (1 + \alpha + \alpha^2) + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$17P = [\alpha + \alpha^2 + \alpha\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$18P = [1 + \alpha + \varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha^2\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$19P = [\alpha + (1 + \alpha)\varepsilon + \alpha^2\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2)\varepsilon : 1]$
$20P = [1 + \alpha + \alpha^2 + (1 + \alpha)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1]$
$21P = [\alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1 + \varepsilon + \alpha\varepsilon^2 : 1]$
$22P = [1 + \alpha + \alpha^2 + \alpha\varepsilon : 1 + (1 + \alpha^2)\varepsilon + (1 + \alpha)\varepsilon^2 : 1]$
$23P = [\alpha + \varepsilon^2 : \alpha^2 + (\alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$24P = [1 + \alpha + (\alpha + \alpha^2)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : \alpha^2 + \varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$25P = [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + \alpha^2\varepsilon^2 : \alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$26P = [1 + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$27P = [\alpha^2 + \alpha^2\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 + (1 + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$28P = [(\alpha + \alpha^2)\varepsilon^2 : 1 : 0]$
$29P = [\alpha^2 + \alpha^2\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 + \alpha^2 + \varepsilon + \varepsilon^2 : 1]$
$30P = [1 + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (1 + \alpha^2)\varepsilon^2 : \alpha + (1 + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1]$
$31P = [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + \alpha^2\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha)\varepsilon + \varepsilon^2 : 1]$
$32P = [1 + \alpha + (\alpha + \alpha^2)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1]$
$33P = [\alpha + \varepsilon^2 : \alpha + \alpha^2 + (\alpha + \alpha^2)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$34P = [1 + \alpha + \alpha^2 + \alpha\varepsilon : \alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (1 + \alpha)\varepsilon^2 : 1]$
$35P = [\alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1 + (1 + \alpha^2)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$36P = [1 + \alpha + \alpha^2 + (1 + \alpha)\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 + (\alpha + \alpha^2)\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$37P = [\alpha + (1 + \alpha)\varepsilon + \alpha^2\varepsilon^2 : \alpha^2 + (\alpha + \alpha^2)\varepsilon + \alpha^2\varepsilon^2 : 1]$
$38P = [1 + \alpha + \varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha^2 + (1 + \alpha^2)\varepsilon : 1]$
$39P = [\alpha + \alpha^2 + \alpha + (\alpha + \alpha^2)\varepsilon^2 : (1 + \alpha + \alpha^2)\varepsilon : 1]$
$40P = [1 + \alpha^2 + (1 + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$41P = [\alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : 1 + \alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1]$
$42P = [\alpha^2\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 : 0]$
$43P = [\alpha^2 + \alpha\varepsilon + \varepsilon^2 : 1 + \alpha^2 + (\alpha + \alpha^2)\varepsilon : 1]$
$44P = [1 + \alpha^2 + (1 + \alpha^2)\varepsilon + \varepsilon^2 : \alpha + (1 + \alpha + \alpha^2)\varepsilon + \alpha^2\varepsilon^2 : 1]$
$45P = [\alpha + \alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2)\varepsilon + (1 + \alpha)\varepsilon^2 : 1]$
$46P = [1 + \alpha + \varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha^2\varepsilon + \varepsilon^2 : 1]$
$47P = [\alpha + (1 + \alpha)\varepsilon + (1 + \alpha)\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2) + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$48P = [1 + \alpha + \alpha^2 + (1 + \alpha)\varepsilon + (1 + \alpha)\varepsilon^2 : \alpha + \alpha^2 + (1 + \alpha^2)\varepsilon + \varepsilon^2 : 1]$
$49P = [\alpha^2\varepsilon + (1 + \alpha^2)\varepsilon^2 : 1 + \varepsilon + \alpha^2\varepsilon^2 : 1]$
$50P = [1 + \alpha + \alpha^2 + \alpha\varepsilon + \alpha^2\varepsilon^2 : 1 + (1 + \alpha^2)\varepsilon + \alpha^2\varepsilon^2 : 1]$
$51P = [\alpha + (\alpha + \alpha^2)\varepsilon^2 : \alpha^2 + (\alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1]$
$52P = [1 + \alpha + (\alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha^2 + \varepsilon + (1 + \alpha)\varepsilon^2 : 1]$
$53P = [\alpha + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : \alpha^2\varepsilon + \alpha\varepsilon^2 : 1]$
$54P = [1 + \alpha^2 + (1 + \alpha + \alpha^2)\varepsilon + (\alpha + \alpha^2)\varepsilon^2 : 1 + \alpha + \alpha^2 + \alpha\varepsilon + (1 + \alpha + \alpha^2)\varepsilon^2 : 1]$
$55P = [\alpha^2 + \alpha^2\varepsilon + \alpha\varepsilon^2 : 1 + (1 + \alpha^2)\varepsilon + \alpha\varepsilon^2 : 1]$
$56P = [0 : 1 : 0]$

- Table of Coding the Elements of G

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

TABLE I
TABLE OF LETTERS

Code of m.P	*Symbol*
001001010101100000100000000	*a*
101111011010101100100000000	*b*
011111011011110001100000000	*c*
110011011111111101100000000	*d*
010000011011011000100000000	*e*
111010001011111000100000000	*f*
000001101100101100100000000	*g*
111110110100011010100000000	*h*
010110110001011001100000000	*i*
110100111001101011100000000	*j*
011010001000111111100000000	*k*
101101100111010101100000000	*l*
001010100100001100100000000	*m*
000001100100000000000000000	*n*
001010001101011100100000000	*o*
101101010010111111100000000	*p*
011010011011101011100000000	*q*
110100011111001011100000000	*r*
010110001011101000100000000	*s*
111110111011101010100000000	*t*
000001101100100010100000000	*u*
111010000100101110100000000	*v*
010000100001011011100000000	*w*
110011111001100101100000000	*x*
011111001000001101100000000	*y*
101111101111010111100000000	*z*
001001111100101011100000000	*(*
000000011100000000000000000	*)*
001001111101100100100000000	*;*
101111101010101010100000000	*!*
011111001011110100100000000	*:*
110011111111111010100000000	*§*
010000100011011111100000000	*.*
111010000011111110100000000	*@*
000001101100101111100000000	*>*
111110111100011101100000000	*<*
010110001001011001100000000	*%*
110100011001101000100000000	*£*
011010011000111000100000000	*$*
101101010111010101100000000	*/*
001010001100001101100000000	*?*
000001111100000000000000000	
001010100101011000100000000	*#*
101101100010111001100000000	*0*
011010001011101110100000000	*1*
110100111111001100100000000	*2*
010110110011101111100000000	*3*
111110110011101100100000000	*4*
000001101100100001100000000	*5*
111010001100101001100000000	*6*
010000011001011011100000000	*7*
110011011001100110100000000	*8*
011111011000001010100000000	*9*
101111011111010111100000000	*,*
001001010100101010100000000	*space*
000000000100000000000000000	*~*

- 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*
001001010101100000100000000	*a*
110011011111111101100000000	*d*
001010100100001100100000000	*m*
000001100100000000000000000	*n*
111110111011101010100000000	*t*
000001101100100010100000000	*u*
111010000100101110100000000	*v*
101111101111010111100000000	*z*
101101100111010101100000000	*l*
010110110001011001100000000	*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:

(101111011010101100100000000,011111011011110001100000000)(110011011111111101100000000,010000011011011000100000000)(111010001011111000100000000,000001101100101100100000000)(111110110100011010100000000,010110110001011001100000000)(110100111001101011100000000,011010001000111111100000000)(101101100111010101100000000,001010100100001100100000000)(000001100100000000000000000,001010001101011100100000000)
(101111011010101100100000000,011111011011110001100000000)(110011011111111101100000000,010000011011011000100000000)(111010001011111000100000000,000001101100101100100000000)(111110110100011010100000000,010110110001011001100000000)(110100111001101011100000000,011010001000111111100000000)(101101100111010101100000000,001010100100001100100000000)(000001100100000000000000000,001010001101011100100000000)

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 $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$ 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.
[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 Mathemathics 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).