Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 50(2), 2023, Pages 313–324, DOI: 10.52846/ami.v50i2.1689
ISSN: 1223-6934

Elliptic Curves over a Finite Ring

Zakariae Cheddour, Abdelhakim Chillali, and Ali Mouhib

Abstract. Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime p such that $p \geq 5$. Let α be a root of a monic polynomial of a minimal degree over $\mathbb{F}_q$. In this paper, we will study elliptic curves over $(\mathbb{F}_q[\alpha], +, *)$, where $+$ is the usual addition and $*$ represent a non-standard product law over $\mathbb{F}_q[\alpha]$. Using elliptic curves over this ring can result in a cryptographic method that is fast, simple and secure.

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G30.
Key words and phrases. Cryptosystem; elliptic curves; keys exchange; finite field; finite ring; local ring.

1. Introduction

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime p such that $p \geq 5$. An elliptic curve $E_{a,b}$ over $\mathbb{F}_q$ is given by the Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, where the coefficients a, b are in $\mathbb{F}_q$.
It is well known that elliptic curves are a versatile cryptographic tool [2, 4, 6, 19, 20, 21, 22, 25], and in particular, that their group structure plays a crucial role in such applications, see [13, 14, 18, 23].
This work follows the series of works that study elliptic curves on finite rings. This study was introduced by M. Virat over the ring $\mathbb{F}_q[e]$, $e^2 = 0$, where q is a prime ≥ 5 [29]. Then the second author A. Chillali develops and generalizes this work to the ring $\mathbb{F}_q[e]$, $e^n = 0$ [9]. In addition, elliptic curves on a local ring of characteristic 3 have been studied by Hassib et al [11]. For the characteristic 2, the study is done by Tadmori et al in [27]. Also, he studied in [25, 26] such curves over a non-local ring. In the same context of a nonlocal ring, Boulbot et al have studied this kind of curve over $\mathbb{F}_q[e]$, $e^3 = e^2$ [4], and over $\mathbb{F}_q[e]$, $e^2 = e$ [5]. In this work, we study elliptic curves defined on the ring $\mathbb{F}_q[\alpha]$, where α is a root of a monic polynomial $P(X)$ of minimal degree denoted by n on $\mathbb{F}_q$. The new advantage of this approach is to obtain a large number of points with a smaller prime p, because we will prove $\sharp E_{a,b}(\mathbb{F}_q[\alpha]) = \prod_{k=0}^{n-1} \sharp E_k$ (Corollary 3.6), in order to reserve memory for the calculations. Moreover, the group law of $E_{a,b}$ is easy to calculate in the forward direction, but difficult in the reverse direction. Thus, in this paper, we will define a non-standard way of multiplying $*$ elements on $\mathbb{F}_q[\alpha]$, as follows, for $X = \sum_{k=0}^{n-1} x_k\alpha^k$, $Y = \sum_{k=0}^{n-1} y_k\alpha^k$, we have

$$X * Y = \sum_{k=0}^{n-1} A_k\alpha^k, \text{ such that } A_0 = x_0y_0,\ A_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$$

Received September 24, 2022. Accepted June 18, 2023.

where P_k and φ_k are a collection of maps from $\mathbb{F}_q[\alpha]$ to $\mathbb{F}_q$ defined as follows:

$$\begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{P_k} & \mathbb{F}_q \\ X & \longmapsto & x_k \end{array} \quad and \quad \begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{\varphi_k} & \mathbb{F}_q \\ X & \longmapsto & \sum_{j=0}^{k} P_j(X) \end{array}.$$

In the rest of this paper, we will use the following notation:

- For $X \in \mathbb{F}_q[\alpha]$, we have $X^{*n} = \underbrace{X * X * ... * X}_{n\ times}$,
- $E_{a,b}$ for an elliptic curve over the ring $(\mathbb{F}_q[\alpha], +, *)$ given by a Weierstrass equation $Y^{*2} * Z = X^{*3} + aX * Z^{*2} + bZ^{*3}$, such that the discriminant $D = 4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{F}_q[\alpha]$.

Another objective of this work is the application of these results in cryptography. We describe here one of the variants of the ElGamal public key encryption scheme [10], the Cramer-Shoup elliptic curve encryption scheme [7]. In the same context of Cramer-Shoup encryption, the second author et al presents a new variant of the Cramer-Shoup public key encryption system on a twisted Hessian curve over the ring $\mathbb{F}_q[\epsilon]$, $\epsilon^4 = 0$ [15]. Since we are working in the ring $\mathbb{F}_q[\alpha]$, the new scheme that we will define on the elliptic curve $E_{a,b}$ has the advantage of having a low complexity cost compared to the elliptic curves over a field.

2. The ring $(\mathbb{F}_q[\alpha], +, *)$

In this section we will give some results concerning the ring $(\mathbb{F}_q[\alpha], +, *)$, which are useful for the rest of this article. We keep the same notation as above. So, let $\mathbb{F}_q[\alpha]$ be the set endowed by the usual addition $X + Y = \sum_{k=0}^{n-1}(x_k + y_k)\alpha^k$, and by the product law $*$, $X * Y = \sum_{k=0}^{n-1} A_k \alpha^k$ where $A_0 = x_0 y_0$, and $A_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$.
We then have the following results.

Lemma 2.1. φ_k is a surjective morphism.

Proof. First we will prove that for each $k \in \{0, ..., n-1\}$, φ_k is a morphism:
Let $X = \sum_{k=0}^{n-1} x_k \alpha^k$ and $Y = \sum_{k=0}^{n-1} y_k \alpha^k$ be two elements of $\mathbb{F}_q[\alpha]$.

- $\varphi_k(X + Y) = \sum_{j=0}^{k} P_j(X + Y) = \sum_{j=0}^{k}(P_j(X) + P_j(Y)) = \sum_{j=0}^{k} P_j(X) + \sum_{j=0}^{k} P_j(Y) = \varphi_k(X) + \varphi_k(Y)$
- For $k = 0$, $\varphi_0(X * Y) = A_0 = x_0 y_0 = \varphi_0(X)\varphi_0(Y)$. Suppose that for $k \in \{0, ..., n-1\}$ $\varphi_{k-1}(X * Y) = \varphi_{k-1}(X)\varphi_{k-1}(Y)$, then we obtain

$$\varphi_k(X * Y) = \varphi_{k-1}(X * Y) + A_k = \varphi_{k-1}(X)\varphi_{k-1}(Y) + x_k\varphi_{k-1}(Y) + y_k\varphi_k(X).$$

On the other hand, for any element s in $\mathbb{F}_q$, we put X=s then we have $\varphi_k(X) = s$ for all $k \in \{0, ..., n-1\}$, hence φ_k is surjective. □

Lemma 2.2. The product law $*$ is well defined.

Proof. We will show respectively, that $*$ is commutative, associative and distributive with respect to the law $+$.
Let X, Y and Z be elements of $\mathbb{F}_q[\alpha]$:

- Put $X*Y=\sum_{k=0}^{n-1}A_k\alpha^k$ and $Y*X=\sum_{k=0}^{n-1}B_k\alpha^k$, we shall prove that $X*Y=Y*X$ this turns out to prove that $A_k=B_k$ for all $k\in\{0,...,n-1\}$.
  This follows immediately that:

$$\begin{aligned}A_k&=P_k(X)\varphi_{k-1}(Y)+P_k(Y)\varphi_k(X)\\&=P_k(X)\varphi_{k-1}(Y)+P_k(Y)\varphi_{k-1}(X)+P_k(Y)P_k(X)=B_k.\end{aligned}$$

- We shall prove that $X*(Y*Z)=(X*Y)*Z$. Put $X*(Y*Z)=\sum_{k=0}^{n-1}C_k\alpha^k$ and $(X*Y)*Z=\sum_{k=0}^{n-1}D_k\alpha^k$.
  We have $C_k=\varphi_k(X*(Y*Z))-\varphi_{k-1}(X*(Y*Z))$ and $D_k=\varphi_k((X*Y)*Z)-\varphi_{k-1}((X*Y)*Z)$.
  Thus, we obtains:

$$\begin{aligned}C_k&=\varphi_k(X*(Y*Z))-\varphi_{k-1}(X*(Y*Z))=\varphi_k(X)\varphi_k(Y*Z)-\varphi_{k-1}(X)\varphi_{k-1}(Y*Z)\\&=\varphi_k(X)\varphi_k(Y)\varphi_k(Z)-\varphi_{k-1}(X)\varphi_{k-1}(Y)\varphi_{k-1}(Z)\\&=\varphi_k(X*Y)\varphi_k(Z)-\varphi_{k-1}(X*Y)\varphi_k(Z)\\&=\varphi_k((X*Y)*Z)-\varphi_{k-1}((X*Y)*Z)\\&=D_k\end{aligned}$$

- Put $X*Y=\sum_{k=0}^{n-1}B_k\alpha^k$ and $X*Z=\sum_{k=0}^{n-1}C_k\alpha^k$, where $B_k=P_k(X)\varphi_{k-1}(Y)+P_k(Y)\varphi_k(X)$ and $C_k=P_k(X)\varphi_{k-1}(Z)+P_k(Z)\varphi_k(X)$.
  So from the definition of $*$ it follows that, $X*(Y+Z)=\sum_{k=0}^{n-1}A_k\alpha^k$,
  where $A_k=P_k(X)\varphi_{k-1}(Y+Z)+P_k(Y+Z)\varphi_k(X)$, then

$$\begin{aligned}A_k&=P_k(X)(\varphi_{k-1}(Y)+\varphi_{k-1}(Z))+(P_k(Y)+P_k(Z))\varphi_k(X)\\&=P_k(X)\varphi_{k-1}(Y)+P_k(X)\varphi_{k-1}(Z)+P_k(Y)\varphi_k(X)+P_k(Z)\varphi_k(X)\end{aligned}$$

  So $A_k=B_k+C_k$.

□

Corollary 2.3.
• The set $\mathbb{F}_q[\alpha]$ endowed by the laws " + " and " * " is a finite unitary commutative ring.
• $\mathbb{F}_q[\alpha]$ is a vector space over $\mathbb{F}_q$ of dimension n, and $(1,\alpha,...,\alpha^{n-1})$ is its basis.

2.1. Inverse elements over $\mathbb{F}_q[\alpha]$. The next proposition characterize the set $(\mathbb{F}_q[\alpha])^\times$ of invertible elements in $\mathbb{F}_q[\alpha]$.

Proposition 2.4. Let $X=\sum_{k=0}^{n-1}x_k\alpha^k\in\mathbb{F}_q[\alpha]$, then $X\in\mathbb{F}_q[\alpha]^\times$ if and only if $\varphi_k(X)\neq 0$ for all $k\in\{0,1,...,n-1\}$. The inverse is given by:

$$X^{-1}=\varphi_0(X)^{-1}-\sum_{k=1}^{n-1}x_k\varphi_{k-1}(X)^{-1}\varphi_k(X)^{-1}\alpha^k$$

Proof. Let X be an invertible element of $\mathbb{F}_q[\alpha]$, then there exists Y in $\mathbb{F}_q[\alpha]$ such that $X*Y=\sum_{k=0}^{n-1}A_k\alpha^k=1$ so for each k such that $1\leq k\leq n-1$, $A_0=1$ and $A_k=0$, then we have $y_0=x_0^{-1}$ and $A_k=\varphi_k(X*Y)-\varphi_{k-1}(X*Y)=0$.
It follows that $\varphi_k(X)\varphi_k(Y)-\varphi_{k-1}(X)\varphi_{k-1}(Y)=0$, then $(\varphi_{k-1}(X)+x_k)(\varphi_{k-1}(Y)+y_k)-\varphi_{k-1}(X)\varphi_{k-1}(Y)=0$.

Therefore $y_k\varphi_{k-1}(X) + x_k\varphi_{k-1}(Y) + x_k y_k = 0$, so $y_k[\varphi_{k-1}(X) + x_k] = -x_k\varphi_{k-1}(Y)$. we get that

$$\begin{cases} y_0 = x_0^{-1}, \\ y_k = -x_k\varphi_k(X)^{-1}\varphi_{k-1}(X)^{-1} \quad 1 \leq k \leq n-1. \end{cases}$$

Then we have

$$Y = X^{-1} = \varphi_0(X)^{-1} - \sum_{k=1}^{n-1} x_k\varphi_{k-1}(X)^{-1}\varphi_k(X)^{-1}\alpha^k.$$

From the above, it follows that X is invertible in $\mathbb{F}_q[\alpha]$ if and only if $\varphi_k(X) \neq 0$ *for all k in* $\{0, 1, ..., n-1\}$.
In the following proposition, we prove that $\mathbb{F}_q[\alpha]$ endowed by the law " $+$ " and " $*$ " is a non local ring. □

Proposition 2.5. $(\mathbb{F}_q[\alpha], +, *)$ is a non local ring.

Proof. Consider $I = \cup_{k=0}^{n-1} I_k$ the set of non invertible elements of $\mathbb{F}_q[\alpha]$ with

$$I_k = \{X \in \mathbb{F}_q[\alpha]/\varphi_k(X) = 0\}$$

We shall prove that the set of non invertible elements over $\mathbb{F}_q[\alpha]$ is not an ideal, so for $a \in \mathbb{F}_q$ let $X = a - a\alpha$, $Y = a\alpha$ two elements of I, then $X + Y = a \in \mathbb{F}_q$, hence the result. □

3. Elliptic curves over $\mathbb{F}_q[\alpha]$

In most situations in this article, we will refer to an elliptic curve, E, by an equation of the form

$$y^2 = x^3 + ax + b,$$

called the Weierstrass equation for E, where a and b are constants. In our case, they are elements of a finite field $\mathbb{F}_q$ or of the ring $\mathbb{F}_q[\alpha]$.
In what follows, we study the elliptic curve $E_{a,b}$ over $\mathbb{F}_q[\alpha]$. For this purpose, we define restrictions E_k of $E_{a,b}$ on the finite field $\mathbb{F}_q$.

3.1. The elliptic curves E_k. In what follows, we will use the following notation, for $a = \sum_{k=0}^{n-1} a_k\alpha^k$ and $b = \sum_{k=0}^{n-1} b_k\alpha^k$ in $\mathbb{F}_q[\alpha]$ we put

$$for\, k \in \{0, 1, ..., n-1\}\ , E_k = \{[X : Y : Z] \in P^2(\mathbb{F}_q)/Y^2Z = X^3 + \varphi_k(a)XZ^2 + \varphi_k(b)Z^3\}$$

and $D_k = 4\varphi_k(a)^3 + 27\varphi_k(b)^2$ is its discriminant.
The following theorem gives a link between $E_{a,b}(\mathbb{F}_q[\alpha])$ and E_k.

Theorem 3.1. Let $\mathbb{F}_q$ be a finite field where $q = p^d$, d is a positive integer, $p \geq 5$ is a prime number, and α be a root of a monic polynomial $P(X)$ of a minimal degree over $\mathbb{F}_q$ denoted by n. Then there exist elliptic curves E_k defined over $\mathbb{F}_q$, for $k \in \{0, ..., n-1\}$, such that

$$E_{a,b}(\mathbb{F}_q[\alpha]) \simeq \prod_{k=0}^{n-1} E_k$$

Lemma 3.2. D is invertible in $\mathbb{F}_q[\alpha]$ if and only if $D_k \neq 0$ for all $k \in \{0, 1, ..., n-1\}$.

Proof. We have $D = 4a^{*3} + 27b^{*2} \in \mathbb{F}_q[\alpha]$ such that $a = \sum_{k=0}^{n-1} a_k\alpha^k$, $b = \sum_{k=0}^{n-1} b_k\alpha^k$ and $D = \sum_{k=0}^{n-1} A_k\alpha^k$. Since $\sum_{j=0}^{k} A_j = \varphi_k(D) = \varphi_k(4a^{*3} + 27b^{*2}) = D_k$, we have $A_k = \varphi_k(D) - \varphi_{k-1}(D) = D_k - D_{k-1}$, so $D = \sum_{k=0}^{n-1} A_k\alpha^k = D_0 + \sum_{k=1}^{n-1}(D_k - D_{k-1})\alpha^k$. From the proof of the proposition 2.4 we deduce that, D is invertible in $\mathbb{F}_q[\alpha]$ if and only if $D_k \neq 0$ for all $k \in \{0, 1, ..., n-1\}$. □

Corollary 3.3. *$E_{a,b}(\mathbb{F}_q[\alpha])$ is an elliptic curve over $\mathbb{F}_q[\alpha]$, if and only if E_k is an elliptic curves over $\mathbb{F}_q$ for all $k \in \{0, ..., n-1\}$.*

The following theorem gives a relation between the elements of $E_{a,b}(\mathbb{F}_q[\alpha])$ and the elements of E_k for all $k \in \{0, ..., n-1\}$.

Theorem 3.4. Let X, Y and Z be elements of $\mathbb{F}_q[\alpha]$, then the following statements are equivalent:

- $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\alpha])$,
- $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$, for all $k \in \{0, 1, ..., n-1\}$.

Proof. Let $[X : Y : Z]$ in $E_{a,b}(\mathbb{F}_q[\alpha]) \subset P^2(\mathbb{F}_q[\alpha])$, then there exist U, V and W in $\mathbb{F}_q[\alpha]$ such that,
$U*X+V*Y+W*Z = 1$. So, $\varphi_k(U*X+V*Y+W*Z) = 1$ for all $k \in \{0, 1, ..., n-1\}$, and then $\varphi_k(U)\varphi_k(X) + \varphi_k(V)\varphi_k(Y) + \varphi_k(W)\varphi_k(Z) = 1$, for all $k \in \{0, 1, ..., n-1\}$ and $[\varphi_k(U) : \varphi_k(V) : \varphi_k(W)]$ belong in $P^2(\mathbb{F}_q)$.
We deduce that $(\varphi_k(X), \varphi_k(Y), \varphi_k(Z)) \neq (0, 0, 0)$ and we have $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$.
Reciprocally, let $[x_k : y_k : z_k]$ in E_k, and put $X = x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\alpha^k$,
$Y = y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\alpha^k$, $Z = z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\alpha^k$.
If X is invertible then $[X : Y : Z] \in P^2(\mathbb{F}_q[\alpha])$. Suppose next, that X is not invertible then there exists $l \in \{0, 1, ..., n-1\}$ such that $\varphi_l(X) = 0$.
Consider the set $I_X = \{l \mid \varphi_l(X) = 0, l \in \{0, 1, ..., n-1\}\}$ and $k = min\, I_X$, then $\varphi_k(X) = 0$. It follows that $\varphi_k(Y) \neq 0$ or $\varphi_k(Z) \neq 0$, because $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$.
Without loss of generality, suppose that $\varphi_k(Y) \neq 0$, and put $T = X + \alpha^k * Y$.
If $k = n-1$, then $\varphi_{n-1}(Y) \neq 0$, thus $T = X + \alpha^{n-1} * Y \in (\mathbb{F}_q[\alpha])^\times$. On the other hand we will distinguish between two cases:
If $\varphi_j(X) \neq -\varphi_j(Y)$, for $k < j \leq n-1$, then we have $T = X + \alpha^k * Y \in (\mathbb{F}_q[\alpha])^\times$.
If there exists $k < j \leq n-1$, such that $\varphi_j(X) = -\varphi_j(Y)$ then $\varphi_j(T) = 0$. Suppose that $j = min\, I_T$ then we have $\varphi_j(X) \neq 0$ or $\varphi_j(Y) \neq 0$ or $\varphi_j(Z) \neq 0$ and we apply the above reasoning to T.
So on until we find an invertible element write in the form of linear combine of X, Y and Z. □

Proposition 3.5. For $i \in \{0, 1, ..., n-1\}$, the mappings $\tilde{\varphi}_i$ is well defined, and given by:

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_q[\alpha]) & \xrightarrow{\tilde{\varphi}_i} & E_i \\ [X : Y : Z] & \longmapsto & [\varphi_i(X) : \varphi_i(Y) : \varphi_i(Z)] \end{array}$$

Proof. According to the previous theorem, we have

$$[\varphi_i(X) : \varphi_i(Y) : \varphi_i(Z)] \in E_i, \ for\ all\ i \in \{0, ..., n-1\}.$$

If $[X:Y:Z]=[A:B:C]$, then there exists $U\in(\mathbb{F}_q[\alpha])^{\times}$ such that: $X=U*A$, $Y=U*B$ and $Z=U*C$, then:

$$\begin{aligned}\widetilde{\varphi_i}\left([X:Y:Z]\right) &= [\varphi_i(X):\varphi_i(Y):\varphi_i(Z)]\\ &= \underbrace{[\varphi_i(U)\varphi_i(A):\varphi_i(U)\varphi_i(B):\varphi_i(U)\varphi_i(C)]}_{\varphi_i(U)\in\mathbb{F}_q^*}\\ &= [\varphi_i(A):\varphi_i(B):\varphi_i(C)]\\ &= \widetilde{\varphi_i}([A:B:C]).\end{aligned}$$

It remains to check that this map is well defined in terms of Weierstrass equation.
Let X, Y, Z, a and b in $\mathbb{F}_q[\alpha]$, so we have $Y^{*2}*Z=\sum_{k=0}^{n-1}A_k\alpha^k$, $X^{*3}=\sum_{k=0}^{n-1}B_k\alpha^k$, $a*X*Z^{*2}=\sum_{k=0}^{n-1}C_k\alpha^k$ and $b*Z^{*3}=\sum_{k=0}^{n-1}T_k\alpha^k$, such that
$A_k=\varphi_k(Y)^2\varphi_k(Z)-\varphi_{k-1}(Y)^2\varphi_{k-1}(Z)$, $B_k=\varphi_k(X)^3-\varphi_{k-1}(X)^3$,
$C_k=\varphi_k(a)\varphi_k(X)\varphi_k(Z)^2-\varphi_{k-1}(a)\varphi_{k-1}(X)\varphi_{k-1}(Z)^2$ and $T_k=\varphi_k(b)\varphi_k(Z)^3-\varphi_{k-1}(b)\varphi_{k-1}(Z)^3$.
We deduce that $Y^{*2}*Z=X^{*3}+a*X*Z^{*2}+b*Z^{*3}$ if and only if $A_k=B_k+C_k+T_k$ for all $k\in\{0,1,...n-1\}$ hence the result. □

Proof of Theorem 3.1. To prove the isomorphism of the theorem, we will first prove that the curve $E_{a,b}(\mathbb{F}_q[\alpha])$ is in bijection with $\prod_{k=0}^{n-1}E_k$. So we consider the mapping $\tilde{\varphi}$ defined by

$$\begin{array}{ccc}E_{a,b}(\mathbb{F}_q[\alpha]) & \xrightarrow{\tilde{\varphi}} & \prod_{k=0}^{n-1}E_k\\ [X:Y:Z] & \longmapsto & \prod_{k=0}^{n-1}[\varphi_k(X):\varphi_k(Y):\varphi_k(Z)]\end{array}$$

- As $\tilde{\varphi}_k$ are well defined, then $\tilde{\varphi}$ is well defined.
- $\tilde{\varphi}$ is a surjective map:
  Let $[x_k:y_k:z_k]\in E_k$, then

$$[X:Y:Z]\in E_{a,b}(\mathbb{F}_q[\alpha])$$

where $X=x_0+\sum_{k=1}^{n-1}(x_k-x_{k-1})\alpha^k$, $Y=y_0+\sum_{k=1}^{n-1}(y_k-y_{k-1})\alpha^k$ and $Z=z_0+\sum_{k=1}^{n-1}(z_k-z_{k-1})\alpha^k$.
So we have:

$$\begin{aligned}&\tilde{\varphi}\left(\left[x_0+\sum_{k=1}^{n-1}(x_k-x_{k-1})\alpha^k:y_0+\sum_{k=1}^{n-1}(y_k-y_{k-1})\alpha^k:z_0+\sum_{k=1}^{n-1}(z_k-z_{k-1})\alpha^k\right]\right)\\ &=\prod_{k=0}^{n-1}[\varphi_k(x_0+\sum_{k=1}^{n-1}(x_k-x_{k-1})\alpha^k):\varphi_k(y_0+\sum_{k=1}^{n-1}(y_k-y_{k-1})\alpha^k):\\ &\quad\varphi_k(z_0+\sum_{k=1}^{n-1}(z_k-z_{k-1})\alpha^k)]\\ &=\prod_{k=0}^{n-1}([x_k:y_k:z_k])\end{aligned}$$

hence $\tilde{\varphi}$ is a surjective mapping.

- It's remains to show that $\tilde{\varphi}$ is injective, for that lets $[X:Y:Z]$ and $[X':Y':Z']$ in $E_{a,b}(\mathbb{F}_q[\alpha])$, where $X=\sum_{k=0}^{n-1}x_k\alpha^k$, $Y=\sum_{k=0}^{n-1}y_k\alpha^k$, $Z=\sum_{k=0}^{n-1}z_k\alpha^k$, $X'=\sum_{k=0}^{n-1}x'_k\alpha^k$, $Y'=\sum_{k=0}^{n-1}y'_k\alpha^k$ and $Z'=\sum_{k=0}^{n-1}z'_k\alpha^k$. Suppose that $[\varphi_k(X):\varphi_k(Y):\varphi_k(Z)]=[\varphi_k(X'):\varphi_k(Y'):\varphi_k(Z')]$, then there exist $\beta_k\in(\mathbb{F}_q)^\times$ for all $k\in\{0,1,...,n-1\}$ such that
$$\begin{cases}\varphi_k(X)=\beta_k\varphi_k(X')\\ \varphi_k(Y)=\beta_k\varphi_k(Y')\\ \varphi_k(Z)=\beta_k\varphi_k(Z')\end{cases}\text{, so }\begin{cases}x_k=\beta_k\varphi_k(X')-\beta_{k-1}\varphi_{k-1}(X')\\ y_k=\beta_k\varphi_k(Y')-\beta_{k-1}\varphi_{k-1}(Y')\\ z_k=\beta_k\varphi_k(Z')-\beta_{k-1}\varphi_{k-1}(Z')\end{cases}.$$
Then we have $\begin{cases}x_k=\beta_kx'_k+(\beta_k-\beta_{k-1})\varphi_{k-1}(X')\\ y_k=\beta_ky'_k+(\beta_k-\beta_{k-1})\varphi_{k-1}(Y')\\ z_k=\beta_kz'_k+(\beta_k-\beta_{k-1})\varphi_{k-1}(Z')\end{cases}$.
Consider $\beta=\beta_0+\sum_{k=1}^{n-1}(\beta_k-\beta_{k-1})\alpha$, it follows that
$$\begin{cases}x_k=P_k(X')\varphi_k(\beta)+P_k(\beta)\varphi_k(X')\\ y_k=P_k(Y')\varphi_k(\beta)+P_k(\beta)\varphi_k(Y')\\ z_k=P_k(Z')\varphi_k(\beta)+P_k(\beta)\varphi_k(Z')\end{cases}.$$
Finally we have $X=\beta*X'$, $Y=\beta*Y'$, $Z=\beta*Z'$ and $\beta\in(\mathbb{F}_q[\alpha])^\times$ then $[X:Y:Z]=[X':Y':Z']$.
Hence $\tilde{\varphi}$ is a bijection.

We can show that the mapping $\tilde{\varphi}^{-1}$ defined by:
$\tilde{\varphi}^{-1}(\prod_{k=0}^{n-1}[x_k:y_k:z_k])=[x_0+\sum_{k=1}^{n-1}(x_k-x_{k-1})\alpha^k:y_0+\sum_{k=1}^{n-1}(y_k-y_{k-1})\alpha^k:z_0+\sum_{k=1}^{n-1}(z_k-z_{k-1})\alpha^k]$
is the inverse of $\tilde{\varphi}$. □

Corollary 3.6. With the same notation as above, we have
$$\sharp E_{a,b}(\mathbb{F}_q[\alpha])=\prod_{k=0}^{n-1}\sharp E_k.$$

Example 3.1. Lets $a=2+3\alpha+\alpha^2-5\alpha^3$, $b=1+2\alpha^2-6\alpha^7+\alpha^{12}$ and α be a root of a monic polynomial of a minimal degree over $\mathbb{F}_{691}$, such that $d^\circ P(X)=13$. So, we have
$card(E_0)=726$, $card(E_1)=714$, $card(E_2)=678$, $card(E_3)=652$, $card(E_4)=652$, $card(E_5)=652$, $card(E_6)=652$, $card(E_7)=732$, $card(E_8)=732$, $card(E_9)=732$, $card(E_{10})=732$, $card(E_{11})=732$ and $card(E_{12})=684$.
In view of $\sharp E_{a,b}=\prod_{k=0}^{12}\sharp E_k$, we obtain
$$\sharp E_{a,b}=912990831561236121689283987194354073 6.$$

To complete the proof of the Theorem 3.1, we will define the group law on $E_{a,b}$, in the following subsection.

3.2. The group law $\star$ over $E_{a,b}$. To define the group law $\star$ over $E_{a,b}$, we use the explicit formulas in the article [3] [pages : 236-238], and since $\tilde{\varphi}$ is bijection we can define $\star$ as follows $P\star Q=\tilde{\varphi}^{-1}(\tilde{\varphi}(P)+\tilde{\varphi}(Q))$ for P, $Q\in E_{a,b}$.

Lemma 3.7. The mapping
$$\begin{array}{ccc}(E_{a,b}(\mathbb{F}_q[\alpha]),\star) & \xrightarrow{\tilde{\varphi}} & (\prod_{k=0}^{n-1}E_k,+)\\ [X:Y:Z] & \longmapsto & \prod_{k=0}^{n-1}[\varphi_k(X):\varphi_k(Y):\varphi_k(Z)]\end{array}$$

is an isomorphism of groups.

Proof. From the previous theorem we have $\tilde{\varphi}$ is a bijection and according to the construction of the group law over $E_{a,b}$ we have

$$\tilde{\varphi}([X:Y:Z]\star[X':Y':Z'])=\tilde{\varphi}([X:Y:Z])+\tilde{\varphi}([X':Y':Z']).$$

So $\tilde{\varphi}$ is an isomorphism of groups. □

Which ends the demonstration of Theorem 3.1.

4. Applications

In cryptography applications, we have:

- If $\sharp E_{a,b}(\mathbb{F}_q[\alpha]) := n$ is an odd number, then $n=\prod_{k=0}^{n-1} n_k$ is the factorization of n, where $n_k := \sharp E_k$, hence the cardinal of $E_{a,b}(\mathbb{F}_q[\alpha])$ is not a prime number.

- **The discrete logarithm problem** [1, 22] in $E_{a,b}(\mathbb{F}_q[\alpha])$ is equivalent to the discrete logarithm problem in $\prod_{k=0}^{n-1} E_k$.

5. Cramer-Shoup Elliptic curve cryptosystem

The Cramer-Shoup cryptosystem for $E_{a,b}$ essentially consists in mapping the operations usually performed in the multiplicative group $\mathbb{Z}_p$ to the set of points of the elliptic curve $E_{a,b}$, endowed with an additive group law.
Alice and **Bob** want to communicate in a secure way, for that they choose the initialization parameters of the Cramer-Shoup elliptic curve cryptosystem,

- A large prime number p, $m, n \in \mathbb{N}^*$.

- A finite ring $\mathbb{F}_q[\alpha]$.

- An elliptic curve $E_{a,b}$ such that $4a^3+27b^2$ is invertible in $\mathbb{F}_q[\alpha]$.

- A point $P \in E_{a,b}$ of large prime order τ and the cyclic group $G=\langle P\rangle$.

5.1. Coding of the elements of G. Let for example $P=[2+8\alpha:10+4\alpha:1]\in E_{1+2\alpha,2}\left(\mathbb{F}_{11}[\alpha]\right)$, P is of order $\tau=104$.
We will use the subgroup $G=<P>$ of $E_{1+2\alpha,2}(\mathbb{F}_{11}[\alpha])$ to encrypt message. Thus, for each element $Q=m\cdot P\in G$, where $m\in\{1,2,\dots\tau\}$, we will give a code.
Let $Q=[\sum_{k=0}^{n} x_k\alpha^k : \sum_{k=0}^{n} y_k\alpha^k : \sum_{k=0}^{n} z_k\alpha^k]$ where, x_k, y_k and z_k are elements of $\mathbb{F}_q$, for $i\in\{0,...,n\}$.
Thus, we code Q as follows:

$$Q=\underbrace{x_0...x_n y_0...y_n z_0...z_n}_{3\times(n+1)}$$

We also attach any element $Q\in G$ with a letter of the alphabet or a punctuation sign.

5.2. Cramer-Shoup $E_{a,b}$ cryptosystem Key generation. The generation of a public key in $E_{a,b}$ is as follows:

- **Alice** chooses five random integers $(c_1,\, c_2,\, s_1,\, s_2,\, x_1,\, x_2) \in (\mathbb{F}_\tau)^5$.
- **Alice** computes $E_1 = c_1P$, $E_2 = c_2P$, $E_3 = s_1P + s_2E_1$, $E_4 = x_1P + x_2E_1$.

Then, the public key is $\{P,\, E_1,\, E_2,\, E_3,\, E_4\}$ and the private key is $(c_1, c_2, s_1, s_2, x_1, x_2)$.

5.2.1. *Encryption of message.* To encrypt a message P_m to **Alice** under her public key $\{P,\, E_1,\, E_2,\, E_3,\, E_4\}$, we use the following statement:

- **Bob** converts the plaintext message P_m to a point $P_m = (X_m, Y_m, Z_m)$ on the elliptic curve $E_{a,b}$ with $X_m \neq 0, Y_m \neq 1, Z_m \neq 0$.
- **Bob** chooses a random $k \in \mathbb{F}_\tau$, and calculates: $W_1 = kP$, $W_2 = kE_1$, $u = kE_2 + P_m$, $\delta = \mathbb{H}(W_1, W_2, u)$ (where $\mathbb{H}()$ is a collision-resistant hash function), $R = kE_3 + k\delta E_4$.
- **Bob** sends the ciphertext (W_1, W_2, u, R) to **Alice**.

5.2.2. *Decryption of message.* To decrypt this message, with **Alice**'s secret key $(c_1,\, c_2,\, s_1,\, s_2,\, x_1,\, x_2)$:

- **Alice** computes $\delta = \mathbb{H}(W_1, W_2, u)$, and verifies that
$$s_1W_1 + s_2W_2 + \delta(x_1W_1 + x_2W_2) = R.$$
If this test fails, further decryption is aborted and the output is rejected.
- Otherwise, **Alice** computes $P_m = u - c_2W_1$. The decryption stage correctly decrypts any properly-formed ciphertext, since
$$u - c_2W_1 = kE_2 + P_m - c_2kP = kc_2P + P_m - wkP = P_m.$$

5.3. Security of this protocol. In this section, we discuss the security and compare it to other schemes.

5.3.1. *Security.* Our system is secure for the following reasons:
• Cramer-Shoup $E_{a,b}$ cryptosystem is directly based on the difficulty of solving the ECDLP over $(G, +)$ of base P. In our system, we have $V_1 = kP$, $V_2 = kQ$, $u = kT + P_m$, $R = kE + k\delta K$ are the public equations. The point $P_m = (X_m, Y_m, Z_m)$ over $E_{a,b}$, the secret integer k and the collision-resistant hash function $\mathbb{H}$ are all private.
• The security analysis of the Cramer-Shoup cryptosystem over $E_{a,b}$ relies on the difficulty of the decisional Diffie-Hellman (DDH) problem, which states that the tuple (nP, mP, nmP) (where P is a base point) is indistinguishable from (nP, mP, eP), where n, m, and e are integers randomly selected.

Remark 5.1. If we assume that we have the following two conditions:
• The hash function $\mathbb{H}$ is chosen in a universal one-way family.
• The Diffie-Hellman decision problem is difficult in the group G.
Then we have the following Lemma.

Lemma 5.1. The above cryptosystem is secure against adaptive chosen ciphertext attack.

Proof. Since we assume that: the hash function $\mathbb{H}$ is chosen in a universal one-way family, and The Diffie-Hellman decision problem is hard in the group G. which feels the same conditions in Theorem 1, [Section 4] [7]. Hence the result. □

5.4. Discussion and analysis. The $E_{a,b}$ version of the Cramer-Shoup cipher is the analog of the Cramer-Shoup cipher [7]. where,

• Multiplication operations replaced by additions.

• Exponentiation operations replaced by multiplication.

Since, ECLDP is hard to solve compared to DLP on fields, we can say that Cramer-Shoup encryption at $E_{a,b}$ is more secure than the original Cramer-Shoup encryption. Moreover, we have sub-exponential algorithms that do DPL resolution over fields. However, the cryptographic primitive used in our scheme is based on the difficulty of DLP. Therefore, to ensure a sufficient level of security, it is necessary to work on large fields, which means that we will increase the transmission costs, the implementation and the computation time.

On the other hand, the Cramer-Shoup encryption over $E_{a,b}$ is preferable to the one over fields, due to the fact that the ECDLP is an exponential problem. In the same context we cite two of the best algorithms in exponential time for solving the ECDLP [16, 17, 22, 24] over an elliptic curve defined over finite fields. The Shanks Baby-Steps Giant-Steps algorithm and Pollard's p-method algorithm.

So, to ensure a maximum security of the cryptographic system, it is necessary to choose well the elliptic curve on which we are going to work. For this reason our elliptic curve $E_{a,b}$ on the ring $\mathbb{F}_q[\alpha]$ is to verify this condition because it increases the time of resolution of the ECDLP because we have shown that $\sharp\left(E_{a,b}(\mathbb{F}_q[\alpha])\right) = \prod_{k=0}^{n-1} \sharp E_k$. Therefore, we can say that the time needed to solve the ECLDP on $E_{a,b}$ is larger than the one for the elliptic curve on a finite field.

The Cramer-Shoup cryptosystem is one a more secure extension of ElGamal cryptosystem. such as the 1st is based on (DDH-A)(Decisional Diffie-Hellman) on the other hand ElGamal cryptosystem is based on (CDH-A)(Computational Diffie-Hellman Assumption). Therefore, we have Cramer-Shoup on $E_{a,b}$ is more secure than ElGamal encryption scheme. On the other hand, among the inconviniant of Cramer-Shoup cryptosystem on $E_{a,b}$ is that the cipher text is longer than the plaintext.

Solving the ECLDP is more difficult than the IFP (Integer Factorization Problem). Thus, the Cramer-Shoup cryptosystem on $E_{a,b}$ is more secure than the RSA cryptosystem. Moreover, ECLDP gives a higher level of security with small keys (in the sense of sizes) than in the RSA or DSA cryptosystem.

Digital Signature Algorithm [8, 10]. The following table shows the length of the key to achieve an appropriate security level of k-bit.

security level	symmetric algorithms	elliptic curve algorithms	asymmetric algorithms like: RSA, DSA and El Gamal
128	80	160	1024
1024	128	256	2048

We conclude that:

• the memory consumption in the Cramer-Shoup cryptosystem over $E_{a,b}$ is much lower than in the Cramer-Shoup signature scheme based on strong RSA [8].

• The size of the message encrypted in the Cramer-Shoup cryptosystem over $E_{a,b}$ is larger than in the RSA-based encryption.

5.5. Conclusion. In this work, we have extended the results for elliptic curves on $\mathbb{F}_q[\alpha]$ and related to elliptic curves over $\mathbb{F}_q$ by the Theorem 3.1. Moreover, we prove that the discrete logarithm problem in $E_{a,b}$ is equivalent to that in E_k. We also

introduce the Cramer-Shoup cryptosystem on $E_{a,b}$ which proves to be more secure than his original cryptosystem [7] and his cryptosystem on elliptic curve [12, 28]. In other respects, it works with smaller key sizes than RSA, but results in a higher ciphertext expansion rate.

Conflict-of-interest statements

All authors declare that they have no conflicts of interest.

References

[1] A. Amadori, F. Pintore, M. Sala, On the discrete logarithm problem for prime-field elliptic curves, *Finite Fields and Their Applicationsx* **51** (2018), 168–182.

[2] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[3] W. Bosma, H.W. Lenstra, Complete System of Two Addition Laws for Elliptic Curves, *Journal of Number Theory* **53** (1995), 229-240.

[4] A. Boulbot, A. Chillali, A. Mouhib, Elliptic curves over the ring $\mathbb{F}_q[e]$, $e^3 = e^2$, *Gulf J. Math* **4** (2016), no. 4, 123-129.

[5] A. Boulbot, A. Chillali, A. Mouhib, Elliptic Curves Over the Ring $\mathbb{R}^*$, *Boletim da Sociedade Paranaense de Matematica* **38** (2020), no. 3, 193-201.

[6] Z. Cheddour, A. Chillali, A. Mouhib, The "Elliptic" matrices and a new kind of cryptography, *Boletim da Sociedade Paranaense de Matematica* **41** (2023).

[7] R. Cramer and V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (eds) *Advances in Cryptology— CRYPTO '98, CRYPTO 1998*, Lecture Notes in Computer Science 1462 (1998), Springer, Berlin, Heidelberg.

[8] R. Cramer, V. Shoup, Signature Schemes Based on the Strong RSA Assumption, *ACM Trans. Inf. Syst. Security* **3** (2000), no. 3, 161-185.

[9] A. Chillali, Ellipic curve over ring, *International Mathematical Forum* **4** (2011), 1501-1505.

[10] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, In: *Advances in Cryptology, CRYPTO 1984*, Lecture Notes in Computer Science 196 (1984), Springer, Berlin, Heidelberg.

[11] M.H. Hassib, A. Chillali, M.A. Elomary, Elliptic curve over a chain ring of characteristic 3, *Journal of Taibah University for Science* **9** (2015), no. 3, 276–287.

[12] M. Gotaishi, S. Tsujii, Organizational Cryptography for Access Control, *IACR Cryptology ePrint Archive* (2018). Available at https://eprint.iacr.org/2018/1120.pdf

[13] A. Grini, A. Chillali, H. Mouanis, Cryptography over twisted Hessian curves of the ring $\mathbb{F}_q[e]$, $e^2 = 0$, *Adv. Math. Sci. J.* **10** (2021), no. 1, 235–243.

[14] A. Grini, A. Chillali, H. Mouanis, The Binary Operations Calculus in $H^2_{a,d}$, Boletim da Sociedade Paranaense de Matematica **40** (2022).

[15] A. Grini, A. Chillali, H. Mouanis, A new cryptosystem based on a twisted Hessian curve $H^4_{a,d}$, *Journal of Applied Mathematics and Computing* **68** (2022), no. 4, 235–243.

[16] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* **48** (1987), no. 177, 203–209.

[17] N. Koblitz, A. Menezes, S. Vanstone, The State of Elliptic Curve Cryptography,*Designs, Codes and Cryptography* **19** (2000), 173-193.

[18] H.W. Lenstra, Elliptic Curves and Number-Theoretic Algorithms, *Proceedings of the International Congress of Mathematicians*, Berkely, California, USA, 1986, 156–163.

[19] M. Ciet, J.J. Quisquater, F. Sica, Compact elliptic curve representations, *J. Math. Cryptol* **5** (2011), 89–100.

[20] V. Miller, Use of elliptic curves in cryptography, In: Williams, H.C. (eds) *Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985*, Lecture Notes in Computer Science 218 (1986), Springer, Berlin, 417–426.

[21] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to a finite field, IEEE Transactions on Information Theory **39** (1993), no. 5, 1639–1646.
[22] A. Odlyzko, Discrete logarithms: the past and the future, *Designs, Codes and Cryptography* **19** (2000), 129–145.
[23] R. Schoof, Elliptic Curves Over finite Fields and the Computation of Square Roots mod p, *Mathematics of Computation* **44**(1985), no. 170, 483–494.
[24] D.R. Stinson, *Cryptography Theory And Practice*, 3rd edition, Chapman Hall/CRC, New York, 2006.
[25] A. Tadmori, A. Chillali, M. Ziane, Cryptography over the elliptic curve $E_{a,b}$, *Journal of Taibah University for Science* **9** (2015), no. 3, 326–331.
[26] A. Tadmori, A. Chillali, M. Ziane, Elliptic curve over ring A^4, *Applied Mathematical Sciences* **9** (2015), no. 35, 1721–1733.
[27] A. Tadmori, A. Chillali, M. Ziane, Elliptic Curves Over a non-local ring $\mathbb{F}_{2^d}[\epsilon]$, $\epsilon^2 = \epsilon$, *Asian-European Journal of Mathematics* **19** (2021), no 3, 2250046.
[28] T.V. Deursen, S. Radomirovic, Insider Attacks and Privacy of RFID Protocols, In: Petkova-Nikova, S., Pashalidis, A., Pernul, G. (eds) *Public Key Infrastructures, Services and Applications. EuroPKI 2011*, Lecture Notes in Computer Science **7163** (2011), Springer, Berlin, Heidelberg, 91–105.
[29] M. Virat, Courbe elliptique sur un anneau et applications cryptographiques, Thése de Doctorat, Université Nice Sophia Antipolis, 2009.

(Zakariae Cheddour) Department of Mathematics, LSI Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, 1223, Morocco
E-mail address: zakariae.cheddour@usmba.ac.ma

(Abdelhakim Chillali) Department of Mathematics, LSI Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, 1223, Morocco
E-mail address: abdelhakim.chillali@usmba.ac.ma

(Ali Mouhib) Department of Mathematics, LSI Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, 1223, Morocco
E-mail address: ali.mouhib@usmba.ac.ma