The quadratic extension extractor for (hyper)elliptic curves in odd characteristic

The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic

Reza Rezaeian Farashahi[1,2] and Ruud Pellikaan[1]

[1] Dept. of Mathematics and Computer Science, TU Eindhoven,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
[2] Dept. of Mathematical Sciences, Isfahan University of Technology,
P.O. Box 85145 Isfahan, Iran
{r.rezaeian, g.r.pellikaan}@tue.nl

Abstract. We propose a simple and efficient deterministic extractor for the (hyper)elliptic curve $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, where q is some power of an odd prime. Our extractor, for a given point P on $\mathcal{C}$, outputs the first $\mathbb{F}_q$-coefficient of the abscissa of the point P. We show that if a point P is chosen uniformly at random in $\mathcal{C}$, the element extracted from the point P is indistinguishable from a uniformly random variable in $\mathbb{F}_q$.

Keywords: Elliptic curve, Hyperelliptic curve, Deterministic extractor.

1 Introduction

A deterministic extractor for a curve is a function that converts a random point on the curve to a bit-string of fixed length that is statistically close to uniformly random. Let $\mathcal{C}$ be an absolutely irreducible nonsingular affine curve that is defined over $\mathbb{F}_{q^2}$, where $q = p^k$, for some odd prime p and positive integer k, by the equation $\mathbf{y}^2 = f(\mathbf{x})$, where the degree of f is an odd number d. In this paper, we propose a simple and efficient deterministic extractor, called `Ext`, for $\mathcal{C}$. Let $\{\alpha_0, \alpha_1\}$ be a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. The extractor `Ext`, for a given point P on $\mathcal{C}$, outputs the *first* $\mathbb{F}_q$-coefficient of the abscissa of the point P. Similarly one could define an extractor that, for a given point on the curve, outputs a $\mathbb{F}_q$-linear combination of $\mathbb{F}_q$-coordinates of the abscissa of the point. Provided that the point P is chosen uniformly at random in $\mathcal{C}$, the element extracted from the point P is indistinguishable from a uniformly random variable in $\mathbb{F}_q$.

Gürel [7] proposed an extractor for an elliptic curve E defined over a quadratic extension of a prime field. Given a point P on $\mathrm{E}(\mathbb{F}_{p^2})$, it extracts half of the bits of the abscissa of P. Provided that the point P is chosen uniformly at random, the statistical distance between the bits extracted from the point P and uniformly random bits is shown to be negligible [7]. We recall this extractor for E in Subsection 5.2 and we improve that result in Theorem 3. The definition of our extractor is similar, yet more general. Our extractor `Ext` is defined for $\mathcal{C}$.

The problem of converting random points of an elliptic curve into random bits has several cryptographic applications. Such applications are key derivation

C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp. 219–236, 2007.

functions, design of cryptographically secure pseudorandom number generators and a class of key exchange protocols based on elliptic curves (e.g, the well-known Elliptic Curve Diffie-Hellman protocol). By the end of the Elliptic Curve Diffie-Hellman protocol, the parties agree on a common secret element of the group, which is indistinguishable from a uniformly random element under the decisional Diffie-Hellman assumption (denoted by DDH). However the binary representation of the common secret element is *distinguishable* from a uniformly random bit-string of the same length. Hence one has to convert this group element into a random-looking bit-string. This can be done using a deterministic extractor.

Kaliski [11] shows that if a point is taken uniformly at random from the union of an elliptic curve and its quadratic twist then the abscissa of this point is uniformly distributed in the finite field. Then Chevassut et al. [3] proposed the TAU technique. This technique allows to extract almost all the bits of the abscissa of a point of the union of an elliptic curve and its quadratic twist. Recently Farashahi et al. [5] proposed two extractors for ordinary elliptic curve E, defined over $\mathbb{F}_{2^N}$, where $N = 2\ell$ and ℓ is a positive integer. For a given point P on E, the first extractor outputs the first $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of P while the second outputs the second $\mathbb{F}_{2^\ell}$-coefficient. They also propose two deterministic extractors for the main subgroup G of E, where E has minimal 2-torsion. If a point P is chosen uniformly at random in G, the bits extracted from the point P are indistinguishable from a uniformly random bit-string of length ℓ.

Sequences of x-coordinates of pseudorandom points on elliptic curves have been studied in [9,12,13,17]. On the other hand, the x-coordinate of a uniformly random point on an elliptic curve can be easily distinguished from uniformly random field element since only about 50% of all field elements are x-coordinates of points of the curve. Our extractors provide only part of the x-coordinate and thereby avoid the obvious problem; the proof shows that actual uniformity is achieved. Our approach is somewhat similar to the basic idea of pseudorandom generators proposed by Gong et al. [6] and Beelen and Doumen [2] in that they use a function that maps the set of points on elliptic curve to a set of smaller cardinality. Our aim is to extract as many bits as possible while keeping the output distribution statistically close to uniform.

We organize the paper as follows. In the next section we introduce some notations and recall some basic definitions. In Section 3, we define an affine variety $\mathcal{A}$ of dimension 2 in $\mathbb{A}^3_{\mathbb{F}_q}$ related to the affine curve $\mathcal{C}$. We show that there exists a bijection between $\mathcal{C}(\mathbb{F}_{q^2})$ and $\mathcal{A}(\mathbb{F}_q)$. Then in Section 4 we propose the extractor $\mathtt{Ext}$ for $\mathcal{C}$ as $\mathtt{Ext}(x, y) = x_0$, where $x = x_0\alpha_0 + x_1\alpha_1$. We show that the output of this extractor, for a given uniformly random point of $\mathcal{C}$, is statistically close to a uniformly random variable in $\mathbb{F}_q$. To show the latter we give bounds on the number of preimages $\mathtt{Ext}^{-1}(x_0)$, where $x_0 \in \mathbb{F}_q$. In fact, by using the bijection between $\mathcal{C}(\mathbb{F}_{q^2})$ and $\mathcal{A}(\mathbb{F}_q)$, we give the estimate for the number of $\mathbb{F}_q$-rational points on the intersection of $\mathcal{A}$ and the hyperplane $\mathbf{x}_0 = x_0$ in $\mathbb{A}^3_{\mathbb{F}_q}$. We show that for almost all values of x_0 in $\mathbb{F}_q$, this intersection is an absolutely

irreducible nonsingular curve. Actually this problem is a special case of Bertini theorems. The classical Bertini theorems say that if an algebraic subvariety $\mathcal{X}$ of $\mathbb{P}^n$ has a certain property, then for a sufficiently general hyperplane $H \subseteq \mathbb{P}^n$, the intersection $H \cap \mathcal{X}$ has the same property (see [8,15]). Then we give two examples in Section 5. We conclude our result in Section 6.

2 Preliminaries

Let us introduce the notations and recall the basic definitions that are used throughout the paper.

Notation. Denote by $\mathbb{Z}_n$ the set of nonnegative integers less than n. A field is denoted by $\mathbb{F}$ and its algebraic closure by $\overline{\mathbb{F}}$. Denote by $\mathbb{F}^*$ the set of nonzero elements of $\mathbb{F}$. The finite field with q elements is denoted by $\mathbb{F}_q$, and its algebraic closure by $\overline{\mathbb{F}}_q$. Let C be a curve defined over $\mathbb{F}_q$, then the set of $\mathbb{F}_q$-rational points on C is denoted by $C(\mathbb{F}_q)$. The cardinality of a finite set S is denoted by $\#S$. We make a distinction between a variable $\mathbf{x}$ and a specific value x in $\mathbb{F}$.

2.1 Finite Field Notation

Consider the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, where $q = p^k$, for some odd prime number p and positive integer k. Then $\mathbb{F}_{q^2}$ is a two dimensional vector space over $\mathbb{F}_q$. Let $\{\alpha_0, \alpha_1\}$ be a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. That means every element x in $\mathbb{F}_{q^2}$ can be represented in the form $x = x_0\alpha_0 + x_1\alpha_1$, where x_0 and x_1 are in $\mathbb{F}_q$. We recall that $\{\alpha_0, \alpha_1\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ if and only if

$$\begin{vmatrix} \alpha_0 & \alpha_1 \\ \alpha_0^q & \alpha_1^q \end{vmatrix} \neq 0.$$

That is equivalent to $\alpha_0, \alpha_1 \in \mathbb{F}_{q^2}^*$ and $\alpha_0^{q-1} \neq \alpha_1^{q-1}$.

Let $\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$ be the Frobenius map defined by $\phi(x) = x^q$. Let $\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q$ be the *trace* function. Then $\mathrm{Tr}(x) = x + \phi(x)$, for $x \in \mathbb{F}_{q^2}$. Let $\mathrm{N} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q$ be the *norm* function. Then $\mathrm{N}(x) = x\phi(x)$, for $x \in \mathbb{F}_{q^2}$.

Remark 1. Let α be a primitive element of $\mathbb{F}_{q^2}$. So every $x \in \mathbb{F}_{q^2}^*$ is a power of α. Then $\mathrm{N}(\alpha)$ is a primitive element of $\mathbb{F}_q$. Let $x \in \mathbb{F}_{q^2}^*$. Then x is a square in $\mathbb{F}_{q^2}$ if and only if $x = \alpha^{2i}$, for some integer i. Similarly $\mathrm{N}(x)$ is a square in $\mathbb{F}_q$ if and only if $\mathrm{N}(x) = (\mathrm{N}(\alpha))^{2i}$, for some integer i. Furthermore $x = \alpha^{2i}$, for some integer i, if and only if $\mathrm{N}(x) = (\mathrm{N}(\alpha))^{2j}$, for some integer j. Obviously $\mathrm{N}(0) = 0$. Therefor x is a square in $\mathbb{F}_{q^2}$ if and only if $\mathrm{N}(x)$ is a square in $\mathbb{F}_q$.

2.2 Hyperelliptic Curves

Definition 1. *An absolutely irreducible nonsingular curve C of genus at least 2 is called* hyperelliptic *if there exists a morphism of degree 2 from C to the projective line.*

Theorem 1. *Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$, where q is odd. Then C has a plane model of the form*

$$\mathbf{y}^2 = f(\mathbf{x}),$$

where f is a square free polynomial and $2g+1 \leq \deg(f) \leq 2g+2$. The plane model is singular at infinity. If $\deg(f) = 2g+1$ then the point at infinity ramifies and C has only one point at infinity. If $\deg(f) = 2g+2$ then C has zero or two $\mathbb{F}_q$-rational points at infinity.

Proof. See [1,4].

2.3 Deterministic Extractor

In our analysis we use the notion of a deterministic extractor, so let us recall it briefly. For general definition of extractors we refer to [16,18].

Definition 2. *Let X and Y be S-valued random variables, where S is a finite set. Then the* statistical distance *$\Delta(X,Y)$ of X and Y is*

$$\Delta(X,Y) = \tfrac{1}{2}\sum_{s\in S} |\Pr[X=s] - \Pr[Y=s]|.$$

Let U_S denote a random variable uniformly distributed on S. We say that a random variable X on S is δ-uniform*, if $\Delta(X,U_S) \leq \delta$.*

Note that if the random variable X is *δ-uniform*, then no algorithm can distinguish X from U_S with advantage larger than δ, that is, for all algorithms $D : S \longrightarrow \{0,1\}$

$$|\Pr[D(X)=1] - \Pr[D(U_S)=1]| \leq \delta.$$

See [14].

Definition 3. *Let S,T be finite sets. Consider the function* $\mathrm{Ext} : S \longrightarrow T$*. We say that* Ext *is a* deterministic (T,δ)-extractor *for S if* $\mathrm{Ext}(U_S)$ *is δ-uniform on T. That means*

$$\Delta(\mathrm{Ext}(U_S), U_T) \leq \delta.$$

In the case that $T = \{0,1\}^k$, we say Ext *is a* δ-deterministic extractor *for S.*

In this paper we consider deterministic $(\mathbb{F}_q,\delta)$-extractors. Observe that, converting random elements of $\mathbb{F}_q$ into random bit strings is a relatively easy problem. For instance, one can represent an element of $\mathbb{F}_q$ by a number in $\mathbb{Z}_q$ and use Algorithm Q_2 from [10], which was presented without analysis. It can actually be shown, however, that Algorithm Q_2 produces on average $n-2$ bits given a uniformly distributed random number $U_{\mathbb{Z}_q}$, where n denotes the bit length of q.

Furthermore, if q is close to a power of 2, that is, $0 \leq (2^n - q)/2^n \leq \delta$ for a small δ, then the uniform element $U_{\mathbb{F}_q}$ is statistically close to n uniformly random bits.

The following simple lemma is a well-known result (the proof can be found, for instance, in [3]).

Lemma 1. *Under the condition that $0 \leq (2^n - q)/2^n \leq \delta$, the statistical distance between $U_{\mathbb{F}_q}$ and U_{2^n} is bounded from above by δ.*

3 Norm Variety

Consider an absolutely irreducible nonsingular affine curve $\mathcal{C}$ defined over $\mathbb{F}_{q^2}$. We define an affine variety $\mathcal{A}$ in $\mathbb{A}^3_{\mathbb{F}_q}$ from the curve $\mathcal{C}$. Then we show that the number of $\mathbb{F}_{q^2}$-rational points on the affine curve $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the affine variety $\mathcal{A}$.

From now on, let $\mathcal{C}$ be an absolutely irreducible nonsingular affine curve that is defined over $\mathbb{F}_{q^2}$ by the equation

$$\mathbf{y}^2 = f(\mathbf{x}), \tag{1}$$

where $f(\mathbf{x}) \in \mathbb{F}_{q^2}[\mathbf{x}]$ is a monic square-free polynomial of odd degree d. Let

$$f(\mathbf{x}) = \mathbf{x}^d + \sum_{i=0}^{d-1} e_i \mathbf{x}^i = \prod_{i=1}^{d} (\mathbf{x} - \lambda_i), \tag{2}$$

where $e_i \in \mathbb{F}_{q^2}$ and $\lambda_i \in \overline{\mathbb{F}}_q$. Then $\lambda_i \neq \lambda_j$, for $i \neq j$, since $f(\mathbf{x})$ is square-free.

Define the variables $\mathbf{x}_0, \mathbf{x}_1$ by $\mathbf{x} = \mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1$. Then there exist two bivariate functions $f_0, f_1 \in \mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1]$, so that

$$f(\mathbf{x}) = f(\mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1) = f_0(\mathbf{x}_0, \mathbf{x}_1)\alpha_0 + f_1(\mathbf{x}_0, \mathbf{x}_1)\alpha_1. \tag{3}$$

Let $\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$ be the Frobenius map defined by $\phi(x) = x^q$. Define the polynomial

$$\overline{f}(\mathbf{x}) = \mathbf{x}^d + \sum_{i=0}^{d-1} \phi(e_i)\mathbf{x}^i. \tag{4}$$

Define $\overline{\mathbf{x}} = \mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1)$. Then

$$\overline{f}(\overline{\mathbf{x}}) = \overline{f}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1)) = f_0(\mathbf{x}_0, \mathbf{x}_1)\phi(\alpha_0) + f_1(\mathbf{x}_0, \mathbf{x}_1)\phi(\alpha_1). \tag{5}$$

Define

$$F(\mathbf{x}_0, \mathbf{x}_1) = f(\mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1)\overline{f}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1)).$$

Then from equations (3) and (5), we have

$$F(\mathbf{x}_0, \mathbf{x}_1) = (f_0(\mathbf{x}_0, \mathbf{x}_1)\alpha_0 + f_1(\mathbf{x}_0, \mathbf{x}_1)\alpha_1)(f_0(\mathbf{x}_0, \mathbf{x}_1)\phi(\alpha_0) + f_1(\mathbf{x}_0, \mathbf{x}_1)\phi(\alpha_1)).$$

We note that f_0, f_1 are in $\mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1]$. Also $\alpha_i\phi(\alpha_i) = \mathrm{N}(\alpha_i) \in \mathbb{F}_q$, for $i \in \{0, 1\}$. Furthermore $\alpha_0\phi(\alpha_1) + \phi(\alpha_0)\alpha_1 = \mathrm{Tr}(\alpha_0)\mathrm{Tr}(\alpha_1) - \mathrm{Tr}(\alpha_0\alpha_1) \in \mathbb{F}_q$. Hence F is a polynomial in $\mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1]$.

Proposition 1. *The polynomial F is square-free.*

Proof. The affine curve $\mathcal{C}$ is defined by the equation $\mathbf{y}^2 = f(\mathbf{x}) = \prod_{i=1}^{d}(\mathbf{x} - \lambda_i)$, where $\lambda_i \in \overline{\mathbb{F}}_q$ and $\lambda_i \neq \lambda_j$, for $i \neq j$. Then

$$f(\mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1) = \prod_{i=1}^{d}(\mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1 - \lambda_i). \tag{6}$$

Hence $f(\mathbf{x}_0\alpha_0+\mathbf{x}_1\alpha_1)$ is a square-free polynomial. Consider the polynomial $\overline{f}(\mathbf{x})$ (see equality (4)). Then $\overline{f}(\mathbf{x}) = \prod_{i=1}^{d}(\mathbf{x}-\phi(\lambda_i))$. Since $\lambda_i \neq \lambda_j$, for $i \neq j$, and ϕ is bijective, so $\phi(\lambda_i) \neq \phi(\lambda_j)$, for $i \neq j$. Hence the polynomial $\overline{f}(\mathbf{x})$ is a square free polynomial. Then

$$\overline{f}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1)) = \prod_{i=1}^{d}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1) - \phi(\lambda_i)). \tag{7}$$

So $\overline{f}(\mathbf{x}_0\phi(\alpha_0)+\mathbf{x}_1\phi(\alpha_1))$ is a square-free polynomial. Now assume that $f(\mathbf{x}_0\alpha_0+\mathbf{x}_1\alpha_1)$ and $\overline{f}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1))$ have a common factor. Then $\phi(\alpha_0) = \gamma\alpha_0$ and $\phi(\alpha_1) = \gamma\alpha_1$, for some $\gamma \in \mathbb{F}_{q^2}$, which is a contradiction, since $\alpha_0\phi(\alpha_1) \neq \phi(\alpha_0)\alpha_1$ (see Subsection 2.1). Therefore $f(\mathbf{x}_0\alpha_0 + \mathbf{x}_1\alpha_1)$ and $\overline{f}(\mathbf{x}_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1))$ do not have a common factor. Thus F is a square-free polynomial.

In particular, Proposition 1 shows that the polynomial F is not a square in $\overline{\mathbb{F}}_q[\mathbf{x}_0, \mathbf{x}_1]$. Consider the polynomial $\mathbf{z}^2 - F(\mathbf{x_0}, \mathbf{x}_1)$ in $\mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1, \mathbf{z}]$. Then this polynomial is absolutely irreducible in $\overline{\mathbb{F}}_q[\mathbf{x}_0, \mathbf{x}_1, \mathbf{z}]$.

Definition 4. *Define the affine variety $\mathcal{A}$ over $\mathbb{F}_q$ by the equation*

$$\mathbf{z}^2 - F(\mathbf{x}_0, \mathbf{x}_1) = 0.$$

The affine variety $\mathcal{A}$ is absolutely irreducible, since the polynomial $\mathbf{z}^2 - F(\mathbf{x_0}, \mathbf{x}_1)$ is absolutely irreducible.

Remark 2. Let $P = (x, y) \in \mathcal{C}(\mathbb{F}_{q^2})$, where $x = x_0\alpha_0 + x_1\alpha_1$ and $x_0, x_1 \in \mathbb{F}_q$. So $y^2 = f(x)$. Then $\phi(y^2) = \phi(f(x)) = \overline{f}(\phi(x)) = \overline{f}(x_0\phi(\alpha_0) + x_1\phi(\alpha_1))$. Let $z = \mathrm{N}(y) = y\phi(y)$. Then

$$z^2 = f(x)\overline{f}(\phi(x)) = f(x_0\alpha_0 + x_1\alpha_1)\overline{f}(x_0\phi(\alpha_0) + x_1\phi(\alpha_1)) = F(x_0, x_1).$$

That means $(x_0, x_1, z) \in \mathcal{A}(\mathbb{F}_q)$.

In Theorem 2, we show that the number of $\mathbb{F}_{q^2}$-rational points on the affine curve $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the affine variety $\mathcal{A}$. For the proof of Theorem 2, we need several lemmas and a proposition.

Lemma 2. *Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}(\mathbb{F}_{q^2}) \longrightarrow \mathbb{A}^2(\mathbb{F}_q)$, by*

$$\pi_{\mathcal{C}}(x, y) = (x_0, x_1),$$

where $x = x_0\alpha_0 + x_1\alpha_1$. Assume that $\pi_{\mathcal{C}}^{-1}(x_0, x_1) \neq \emptyset$. If $F(x_0, x_1) = 0$, then $\#\pi_{\mathcal{C}}^{-1}(x_0, x_1) = 1$, otherwise $\#\pi_{\mathcal{C}}^{-1}(x_0, x_1) = 2$.

Proof. Let $P = (x, y) \in \pi_{\mathcal{C}}^{-1}(x_0, x_1)$, where $x = x_0\alpha_0 + x_1\alpha_1$. Remark 2 shows that $(\mathrm{N}(y))^2 = F(x_0, x_1)$. So $F(x_0, x_1) = 0$ if and only if $y = 0$. If $y = 0$, then $\pi_{\mathcal{C}}^{-1}(x_0, x_1) = \{(x, 0)\}$. If $y \neq 0$, then $-P = (x, -y) \in \pi_{\mathcal{C}}^{-1}(x_0, x_1)$ and $-P \neq P$. Since $P, -P$ are the only points on $\mathcal{C}(\mathbb{F}_{q^2})$, with the fixed first coordinate x, then $\pi_{\mathcal{C}}^{-1}(x_0, x_1) = \{P, -P\}$.

Lemma 3. *Define the projection map* $\pi_{\mathcal{A}} : \mathcal{A}(\mathbb{F}_q) \longrightarrow \mathbb{A}^2(\mathbb{F}_q)$, *by*

$$\pi_{\mathcal{A}}(x_0, x_1, z) = (x_0, x_1).$$

Assume $\pi_{\mathcal{A}}^{-1}(x_0, x_1) \neq \emptyset$. *If* $F(x_0, x_1) = 0$, *then* $\#\pi_{\mathcal{A}}^{-1}(x_0, x_1) = 1$, *otherwise* $\#\pi_{\mathcal{A}}^{-1}(x_0, x_1) = 2$.

Proof. Let $(x_0, x_1, z) \in \pi_{\mathcal{A}}^{-1}(x_0, x_1)$. Then $z^2 = F(x_0, x_1)$. If $F(x_0, x_1) = 0$, then $z = 0$ and $\pi_{\mathcal{A}}^{-1}(x_0, x_1) = \{(x_0, x_1, 0)\}$. If $F(x_0, x_1) \neq 0$, then (x_0, x_1, z) and $(x_0, x_1, -z)$ are the only points on $\mathcal{A}$, such that they have the first and second coordinates equal x_0 and x_1. Furthermore $z \neq -z$. Therefore in this case $\pi_{\mathcal{A}}^{-1}(x_0, x_1) = \{(x_0, x_1, z), (x_0, x_1, -z)\}$.

Proposition 2. *For all* $x_0, x_1 \in \mathbb{F}_q$, $\#\pi_{\mathcal{C}}^{-1}(x_0, x_1) = \#\pi_{\mathcal{A}}^{-1}(x_0, x_1)$.

Proof. First assume that $\pi_{\mathcal{C}}^{-1}(x_0, x_1) \neq \emptyset$. Then there exists a point (x, y) on $\mathcal{C}(\mathbb{F}_{q^2})$, such that $x = x_0\alpha_0 + x_1\alpha_1$. Let $z = \mathrm{N}(y)$. Then Remark 2 shows that $(x_0, x_1, z) \in \mathcal{A}(\mathbb{F}_q)$. Therefore $(x_0, x_1, z) \in \pi_{\mathcal{A}}^{-1}(x_0, x_1)$ and $\pi_{\mathcal{A}}^{-1}(x_0, x_1) \neq \emptyset$.

Second assume that $\pi_{\mathcal{A}}^{-1}(x_0, x_1) \neq \emptyset$. Then there exists a point (x_0, x_1, z) on $\mathcal{A}(\mathbb{F}_q)$. Thus $z^2 = F(x_0, x_1)$. Let $x = x_0\alpha_0 + x_1\alpha_1$. Then from Remark 2, $z^2 = f(x)\phi(f(x)) = \mathrm{N}(f(x))$. So $\mathrm{N}(f(x))$ is a square in $\mathbb{F}_q$. Remark 1 implies $f(x)$ is a square in $\mathbb{F}_{q^2}$. Let $y^2 = f(x)$, where $y \in \mathbb{F}_{q^2}$. So $(x, y) \in \mathcal{C}(\mathbb{F}_{q^2})$. That means $(x, y) \in \pi_{\mathcal{C}}^{-1}(x_0, x_1)$ and $\pi_{\mathcal{C}}^{-1}(x_0, x_1) \neq \emptyset$.

Hence $\pi_{\mathcal{A}}^{-1}(x_0, x_1) \neq \emptyset$ if and only if $\pi_{\mathcal{C}}^{-1}(x_0, x_1) \neq \emptyset$. Then Lemmas 2 and 3 conclude the proof of this proposition.

Theorem 2. *The number of* $\mathbb{F}_{q^2}$*-rational points on the affine curve* $\mathcal{C}$ *equals the number of* $\mathbb{F}_q$*-rational points on the affine variety* $\mathcal{A}$.

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = \#\mathcal{A}(\mathbb{F}_q).$$

Proof. Consider the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{A}}$ from Lemmas 2 and 3. Then

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = \sum_{(x_0,x_1)\in\mathbb{A}^2(\mathbb{F}_q)} \#\pi_{\mathcal{C}}^{-1}(x_0, x_1),$$

and

$$\#\mathcal{A}(\mathbb{F}_q) = \sum_{(x_0,x_1)\in\mathbb{A}^2(\mathbb{F}_q)} \#\pi_{\mathcal{A}}^{-1}(x_0, x_1).$$

Proposition 2 shows that $\#\pi_{\mathcal{C}}^{-1}(x_0, x_1) = \#\pi_{\mathcal{A}}^{-1}(x_0, x_1)$, for all $x_0, x_1 \in \mathbb{F}_q$. So the proof of this theorem is completed.

Remark 3. In fact, one can show that the number of $\mathbb{F}_{q^2}$-rational points on the nonsingular projective model of $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the projective closure of $\mathcal{A}$ in $\mathbb{P}^3_{\mathbb{F}_q}$.

4 The Quadratic Extension Extractor

In this section we introduce an extractor that works for the affine curve $\mathcal{C}$ as defined in Section 3. We recall that $\mathcal{C}$ is defined over the quadratic extension of $\mathbb{F}_q$. The extractor, for a given point on the curve, outputs the *first* $\mathbb{F}_q$-coordinate of the abscissa of the point. Then, we show that the output of this extractor, for a given uniformly random point of $\mathcal{C}$, is statistically close to a uniform random variable in $\mathbb{F}_q$.

Similarly one could define an extractor that, for a given point on the curve, outputs a $\mathbb{F}_q$-linear combination of $\mathbb{F}_q$-coordinates of the abscissa of the point. In more detail , let $a_0, a_1 \in \mathbb{F}_q$ be such that both are not zero. The extractor, for a given point $P = (x, y) \in \mathcal{C}(\mathbb{F}_{q^2})$, where $x = x_0\alpha_0 + x_1\alpha_1$, outputs $a_0x_0 + a_1x_1$. Interchange the basis α_0, α_1 to another basis $\widehat{\alpha}_0, \widehat{\alpha}_1$, by

$$\begin{pmatrix} \hat{\alpha}_0 \\ \hat{\alpha}_1 \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix},$$

where $b_0, b_1 \in \mathbb{F}_q$, such that the transformation matrix is nonsingular. Then x can be represented in the form $x = \hat{x}_0\hat{\alpha}_0 + \hat{x}_1\hat{\alpha}_1$, where $\hat{x}_0, \hat{x}_1 \in \mathbb{F}_q$. Clearly $\hat{x}_0 = a_0x_0 + a_1x_1$. This amounts to the extractor that outputs x_0. So without loss of generality we consider the first extractor.

4.1 The Extractor for $\mathcal{C}$

In this subsection we define the extractor for the affine curve $\mathcal{C}$ defined over $\mathbb{F}_{q^2}$ (see Section 3 equation (1)). Then we compute the number of pre-images of this extractor for an element x_0 in $\mathbb{F}_q$, in terms of the number of $\mathbb{F}_q$-rational points on a curve $\mathcal{A}_{x_0}$. In other words, we show some bounds for the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{C}$, whose abscissa have the fixed first $\mathbb{F}_q$-coordinate.

Definition 5. *The extractor* `Ext` *is defined as a function*

$$\begin{aligned} \texttt{Ext} : \mathcal{C}(\mathbb{F}_{q^2}) &\longrightarrow \mathbb{F}_q \\ \texttt{Ext}(x, y) &= x_0, \end{aligned}$$

Theorem 3 gives some bounds for $\#\texttt{Ext}^{-1}(x_0)$, for all x_0 in $\mathbb{F}_q$. For the proof of this theorem, we need several lemmas and propositions. We define the affine curve $\mathcal{A}_{x_0}$ as the intersection of the affine variety $\mathcal{A}$ and the hyperplane $\mathbf{x}_0 = x_0$, for x_0 in $\mathbb{F}_q$. Then in Proposition 3 we show that $\#\mathcal{A}_{x_0}(\mathbb{F}_q) = \#\texttt{Ext}^{-1}(x_0)$, for all x_0 in $\mathbb{F}_q$. We show that the curve $\mathcal{A}_{x_0}$ is reducible if and only if $x_0 \in \mathcal{I}$ (Proposition 4) and the curve $\mathcal{A}_{x_0}$ is singular if and only if $x_0 \in \mathcal{S}$ (Proposition 5), where the sets $\mathcal{I}, \mathcal{S}$ are defined by Definition 9. If the curve $\mathcal{A}_{x_0}$ is absolutely irreducible and singular, we consider the curve $\mathcal{X}_{x_0}$, that is a nonsingular plane model of $\mathcal{A}_{x_0}$. By using the Hasse-Weil bound for the curve $\mathcal{X}_{x_0}$, we obtain the bound for $\#\mathcal{A}_{x_0}(\mathbb{F}_q)$, where $x_0 \notin \mathcal{I}$ (Proposition 8). Note that we have a trivial bound for $\#\mathcal{A}_{x_0}(\mathbb{F}_q)$, if $x_0 \in \mathcal{I}$. Then Proposition 3 concludes the proof of Theorem 3.

Consider the affine variety $\mathcal{A}$ over $\mathbb{F}_q$, as introduced in Definition 4. Fix the element x_0 in $\mathbb{F}_q$. Then the points of $\mathcal{A}$ that have the first coordinate equal to x_0 form a curve which we call $\mathcal{A}_{x_0}$.

Definition 6. *Let $x_0 \in \mathbb{F}_q$. The affine curve $\mathcal{A}_{x_0}$ is defined by the equation*

$$F_{x_0}(\mathbf{x}_1, \mathbf{z}) = \mathbf{z}^2 - F_{x_0}(\mathbf{x}_1) = 0,$$

where $F_{x_0}(\mathbf{x}_1) = F(x_0, \mathbf{x}_1)$.

Therefore

$$\mathcal{A}_{x_0}(\mathbb{F}_q) = \{P = (x_1, z) : x_1, z \in \mathbb{F}_q,\ z^2 = F_{x_0}(x_1) = F(x_0, x_1)\}.$$

Note that $\mathbf{x}_1$ and $\mathbf{z}$ are variables and x_0 is a fixed element in $\mathbb{F}_q$.

Proposition 3. *$\#\mathcal{A}_{x_0}(\mathbb{F}_q) = \#\mathtt{Ext}^{-1}(x_0)$, for all x_0 in $\mathbb{F}_q$.*

Proof. Let $x_0 \in \mathbb{F}_q$. Consider the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{A}}$ from Lemmas 2 and 3. Then

$$\#\mathcal{A}_{x_0}(\mathbb{F}_q) = \sum_{x_1 \in \mathbb{F}_q} \#\pi_{\mathcal{A}}^{-1}(x_0, x_1),$$

and

$$\#\mathtt{Ext}^{-1}(x_0) = \sum_{x_1 \in \mathbb{F}_q} \#\pi_{\mathcal{C}}^{-1}(x_0, x_1).$$

Proposition 2 shows that $\#\pi_{\mathcal{C}}^{-1}(x_0, x_1) = \#\pi_{\mathcal{A}}^{-1}(x_0, x_1)$, for all $x_0, x_1 \in \mathbb{F}_q$. So the proof of this proposition is completed.

Remark 4. Let $x_0 \in \mathbb{F}_q$. Define

$$f_{x_0}(\mathbf{x}_1) = f(x_0\alpha_0 + \mathbf{x}_1\alpha_1),$$
$$\overline{f}_{x_0}(\mathbf{x}_1) = \overline{f}(x_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1)).$$

We recall that $F_{x_0}(\mathbf{x}_1) = f_{x_0}(\mathbf{x}_1)\overline{f}_{x_0}(\mathbf{x}_1)$. Note that $f_{x_0}, \overline{f}_{x_0}$ are polynomials in $\mathbb{F}_{q^2}[\mathbf{x}_1]$ and F_{x_0} is a polynomial in $\mathbb{F}_q[\mathbf{x}_1]$. From equalities (6) and (7), we have

$$f_{x_0}(\mathbf{x}_1) = \prod_{i=1}^{d}(x_0\alpha_0 + \mathbf{x}_1\alpha_1 - \lambda_i),$$
$$\overline{f}_{x_0}(\mathbf{x}_1) = \prod_{i=1}^{d}(x_0\phi(\alpha_0) + \mathbf{x}_1\phi(\alpha_1) - \phi(\lambda_i)).$$

Definition 7. *Let $x_0 \in \mathbb{F}_q$. Define $\theta_i = \frac{\lambda_i - x_0\alpha_0}{\alpha_1}$, for $i \in \{1, 2, \ldots, d\}$.*

Then $\phi(\theta_i) = \frac{\phi(\lambda_i) - x_0\phi(\alpha_0)}{\phi(\alpha_1)}$. Furthemore

$$f_{x_0}(\mathbf{x}_1) = \alpha_1^d \prod_{i=1}^{d}(\mathbf{x}_1 - \theta_i),$$
$$\overline{f}_{x_0}(\mathbf{x}_1) = \alpha_1^{qd} \prod_{i=1}^{d}(\mathbf{x}_1 - \phi(\theta_i)).$$

Since $\lambda_i \neq \lambda_j$, for $i \neq j$, so $\theta_i \neq \theta_j$ and $\phi(\theta_i) \neq \phi(\theta_j)$, for $i \neq j$. Thus f_{x_0} and $\overline{f}_{x_0}$ are square free polynomials in $\overline{\mathbb{F}}_q[\mathbf{x}_1]$. Then

$$F_{x_0}(\mathbf{x}_1) = (\mathrm{N}(\alpha_1))^d \prod_{i=1}^{d}((\mathbf{x}_1 - \theta_i)(\mathbf{x}_1 - \phi(\theta_i)).$$

Lemma 4. *$F_{x_0}(\mathbf{x}_1)$ has $\theta \in \overline{\mathbb{F}}_q$ as multiple root if and only if*

$$f_0(x_0, \theta) = f_1(x_0, \theta) = 0.$$

Proof. From Remark 4 and equalities (3), (5), we have

$$\begin{aligned} f_{x_0}(\mathbf{x}_1) &= f_0(x_0, \mathbf{x}_1)\alpha_0 + f_1(x_0, \mathbf{x}_1)\alpha_1, \\ \overline{f}_{x_0}(\mathbf{x}_1) &= f_0(x_0, \mathbf{x}_1)\phi(\alpha_0) + f_1(x_0, \mathbf{x}_1)\phi(\alpha_1), \end{aligned} \tag{8}$$

where $f_0(x_0, \mathbf{x}_1)$ and $f_1(x_0, \mathbf{x}_1)$ are polynomials in $\mathbb{F}_q[\mathbf{x}_1]$. The polynomials f_{x_0} and $\overline{f}_{x_0}$ are square free, so if $(\mathbf{x}_1 - \theta)^2$ is a factor of $F_{x_0}(\mathbf{x}_1)$, then $(\mathbf{x}_1 - \theta)$ is a common factor of both polynomials f_{x_0} and $\overline{f}_{x_0}$. Hence

$$\begin{pmatrix} f_0(x_0, \theta) & f_1(x_0, \theta) \end{pmatrix} \begin{pmatrix} \alpha_0 & \phi(\alpha_0) \\ \alpha_1 & \phi(\alpha_1) \end{pmatrix} = \begin{pmatrix} 0 & 0 \end{pmatrix}.$$

Since the matrix is nonsingular (see Subsection 2.1), so $f_0(x_0, \theta) = f_1(x_0, \theta) = 0$. Converse is obvious.

Definition 8. *For $x_0 \in \mathbb{F}_q$, let*

$$S_{x_0} = \{x_1 \in \overline{\mathbb{F}}_q : f_0(x_0, x_1) = f_1(x_0, x_1) = 0\}$$

and $d_{x_0} = \#S_{x_0}$, $g_{x_0}(\mathbf{x}_1) = \gcd(f_0(x_0, \mathbf{x}_1), f_1(x_0, \mathbf{x}_1))$.

Since $f_{x_0}(\mathbf{x}_1)$ is square free in $\overline{\mathbb{F}}_q[\mathbf{x}_1]$, it follows from equality (8) that g_{x_0} has no multiple root in $\overline{\mathbb{F}}_q$. That means $d_{x_0} = \deg(g_{x_0})$. Furthermore $0 \leq d_{x_0} \leq d$.

Remark 5. From the proof of Lemma 4, $f_{x_0}(x_1) = \overline{f}_{x_0}(x_1) = 0$, for $x_1 \in \overline{\mathbb{F}}_q$, if and only if $f_0(x_0, x_1) = f_1(x_0, x_1) = 0$. So $x_1 \in S_{x_0}$ if and only if $x_1 = \theta_i = \phi(\theta_j)$, for some indexes i and j (see Remark 4). In other words

$$S_{x_0} = \{\theta_1, \theta_2, \ldots, \theta_d\} \cap \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\}.$$

Definition 9. *For $i, j \in \{1, 2, \ldots, d\}$, let*

$$s_{i,j} = \frac{\begin{vmatrix} \lambda_i & \alpha_1 \\ \phi(\lambda_j) & \phi(\alpha_1) \end{vmatrix}}{\begin{vmatrix} \alpha_0 & \alpha_1 \\ \phi(\alpha_0) & \phi(\alpha_1) \end{vmatrix}}.$$

Let $\mathcal{S} = \{s \in \mathbb{F}_q : s = s_{i,j}, \text{ for some indexes } i, j\}$ and $\mathcal{I} = \{s \in \mathcal{S} : d_s = d\}$.

Remark 6. Let $\theta_i = \phi(\theta_j)$, for some indexes i, j. Then

$$\frac{\lambda_i - x_0\alpha_0}{\alpha_1} = \frac{\phi(\lambda_j) - x_0\phi(\alpha_0)}{\phi(\alpha_1)}.$$

Thus

$$x_0 = \frac{\lambda_i\phi(\alpha_1) - \phi(\lambda_j)\alpha_1}{\alpha_0\phi(\alpha_1) - \phi(\alpha_0)\alpha_1} = s_{i,j}.$$

We note that $\alpha_0\phi(\alpha_1) - \phi(\alpha_0)\alpha_1 \neq 0$ (see Subsection 2.1).

The converse is also true. That means $x_0 = s_{i,j}$ if and only if $\theta_i = \phi(\theta_j)$. Furthermore

$$d_{x_0} = \#\{(i,j) : s_{i,j} = x_0\}.$$

So $x_0 \notin \mathcal{S}$ if an only if $d_{x_0} = 0$.

Proposition 4. *The affine plane curve $\mathcal{A}_{x_0}$ is absolutely irreducible if and only if $x_0 \notin \mathcal{I}$.*

Proof. The affine curve $\mathcal{A}_{x_0}$ is defined by the equation $\mathbf{z}^2 = F_{x_0}(\mathbf{x}_1)$. The curve $\mathcal{A}_{x_0}$ is reducible if and only if F_{x_0} is a square in $\overline{\mathbb{F}}_q[\mathbf{x}_1]$. From equality (**??**) F_{x_0} is a square in $\overline{\mathbb{F}}_q[\mathbf{x}_1]$ if and only if $\{\theta_1, \theta_2, \ldots, \theta_d\} = \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\}$. Remarks 5 and 6 explain that this is equivalent to $d_{x_0} = d$.

Remark 7. Assume the affine curve $\mathcal{A}_{x_0}$ is reducible. So from the proof of Proposition 4 we have, $\{\theta_1, \theta_2, \ldots, \theta_d\} = \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\}$. Then $\sum_{i=1}^{d} \theta_i = \sum_{i=1}^{d} \phi(\theta_i)$. Therefore

$$\sum_{i=1}^{d} \frac{\lambda_i - x_0\alpha_0}{\alpha_1} = \sum_{i=1}^{d} \frac{\phi(\lambda_i) - x_0\phi(\alpha_0)}{\phi(\alpha_1)}.$$

Because $\sum_{i=1}^{d} \lambda_i = e_{d-1}$ (see equation (2)), we have

$$dx_0 = \frac{e_{d-1}\phi(\alpha_1) - \phi(e_{d-1})\alpha_1}{\alpha_0\phi(\alpha_1) - \phi(\alpha_0)\alpha_1}.$$

In other words, if $x_0 \in \mathcal{I}$, then

$$dx_0 = \frac{\begin{vmatrix} e_{d-1} & \alpha_1 \\ \phi(e_{d-1}) & \phi(\alpha_1) \end{vmatrix}}{\begin{vmatrix} \alpha_0 & \alpha_1 \\ \phi(\alpha_0) & \phi(\alpha_1) \end{vmatrix}}.$$

Note that the converse is not true. If d is not divisible by p, then $\#\mathcal{I} \leq 1$. Otherwise $\#\mathcal{I} \leq d$.

Proposition 5. *The affine curve $\mathcal{A}_{x_0}$ is singular if and only if $x_0 \in \mathcal{S}$. The curve $\mathcal{A}_{x_0}$ has d_{x_0} singular points.*

Proof. The point $(x_1, z) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ is a singular point on $\mathcal{A}_{x_0}$ if and only if $z = 0$ and x_1 is a double root of $F_{x_0}(\mathbf{x}_1)$. From Lemma 4, x_1 is a double root of $F_{x_0}(\mathbf{x}_1)$ if and only if $x_1 \in S_{x_0}$. So $\mathcal{A}_{x_0}$ has d_{x_0} singular points. Remarks 5 and 6 explain that there exists $x_1 \in S_{x_0}$ if and only if $x_0 = s_{i,j}$, for some indexes i, j. Since $x_0 \in \mathbb{F}_q$, therefore $x_0 \in \mathcal{S}$ if and only if $\mathcal{A}_{x_0}$ is singular.

We recall that g_{x_0} is a square free polynomial of degree d_{x_0} in $\mathbb{F}_q[\mathbf{x}_1]$. From Lemma 4 and Remark 5, g_{x_0} is the square factor of F_{x_0}. Let

$$F_{x_0}(\mathbf{x}_1) = g_{x_0}^2(\mathbf{x}_1) H_{x_0}(\mathbf{x}_1),$$

where H_{x_0} is a square free polynomial of degree $2(d - d_{x_0})$ in $\mathbb{F}_q[\mathbf{x}_1]$.

Definition 10. *Let $\mathcal{X}_{x_0}$ be the affine curve given by the equation*

$$\mathbf{w}^2 - H_{x_0}(\mathbf{x}_1) = 0.$$

Proposition 6. *The affine curve $\mathcal{X}_{x_0}$ is absolutely irreducible and nonsingular if and only if $x_0 \notin \mathcal{I}$.*

Proof. The affine curve $\mathcal{X}_{x_0}$ is defined by the equation $\mathbf{w}^2 = H_{x_0}(\mathbf{x}_1)$. Since H_{x_0} is a square free polynomial of degree $2(d - d_{x_0})$ in $\mathbb{F}_q[\mathbf{x}_1]$, it is absolutely irreducible and nonsingular if and only if H_{x_0} is not constant. Clearly H_{x_0} is constant if and only if $d_{x_0} = d$. That means H_{x_0} is constant if and only if $x_0 \in \mathcal{I}$.

Remark 8. If H_{x_0} is not constant, the affine curve $\mathcal{X}_{x_0}$ is a nonsingular plane model of $\mathcal{A}_{x_0}$.

Proposition 7. *For $x_0 \in \mathbb{F}_q$, $|\#\mathcal{A}_{x_0}(\mathbb{F}_q) - \#\mathcal{X}_{x_0}(\mathbb{F}_q)| \leq d_{x_0}$.*

Proof. The affine curves $\mathcal{A}_{x_0}$ and $\mathcal{X}_{x_0}$ are defined by the equations $\mathbf{z}^2 = F_{x_0}(\mathbf{x}_1)$ and $\mathbf{w}^2 = H_{x_0}(\mathbf{x}_1)$ respectively. We recall that $F_{x_0}(\mathbf{x}_1) = g_{x_0}^2(\mathbf{x}_1) H_{x_0}(\mathbf{x}_1)$. Define the projection maps $\pi_{\mathcal{A}} : \mathcal{A}_{x_0}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, by $\pi_{\mathcal{A}}(x_1, z) = x_1$ and $\pi_{\mathcal{X}} : \mathcal{X}_{x_0}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, by $\pi_{\mathcal{X}}(x_1, w) = x_1$.

Let $x_1 \in \mathbb{F}_q$. First assume that $g_{x_0}(x_1) \neq 0$. Then

$$\#\pi_{\mathcal{A}}^{-1}(x_1) = \#\pi_{\mathcal{X}}^{-1}(x_1) = \begin{cases} 0, & \text{if } H_{x_0}(x_1) \text{ is a non-square in } \mathbb{F}_q, \\ 1, & \text{if } H_{x_0}(x_1) = 0, \\ 2, & \text{if } H_{x_0}(x_1) \text{ is a square in } \mathbb{F}_q^*. \end{cases}$$

Now assume that $g_{x_0}(x_1) = 0$. Then $\#\pi_{\mathcal{A}}^{-1}(x_1) = 1$ and $\#\pi_{\mathcal{X}}^{-1}(x_1)$ equals 0 or 2. Then

$$\begin{aligned} |\#\mathcal{A}_{x_0}(\mathbb{F}_q) - \#\mathcal{X}_{x_0}(\mathbb{F}_q)| &= \left| \sum_{x_1 \in \mathbb{F}_q} \#\pi_{\mathcal{A}}^{-1}(x_1) - \sum_{x_1 \in \mathbb{F}_q} \#\pi_{\mathcal{X}}^{-1}(x_1) \right| \\ &= \sum_{x_1 \in \mathbb{F}_q \,,\, g_{x_0}(x_1) = 0} 1 \leq d_{x_0}. \end{aligned}$$

Proposition 8. *Let $x_0 \in \mathbb{F}_q$. If $x_0 \notin \mathcal{I}$, then*

$$|\#\mathcal{A}_{x_0}(\mathbb{F}_q) - q| \leq 2(d - d_{x_0} - 1)\sqrt{q} + d_{x_0} + 1.$$

Proof. Let $x_0 \in \mathbb{F}_q \setminus \mathcal{I}$. Then the affine curve $\mathcal{X}_{x_0}$ is absolutely irreducible and nonsingular (see Proposition 6). The degree of $\mathcal{X}_{x_0}$ is $2(d - d_{x_0})$. Let $\widetilde{\mathcal{X}}_{x_0}$ be the nonsingular projective model of $\mathcal{X}_{x_0}$. So $\widetilde{\mathcal{X}}_{x_0}$ is a hyperelliptic curve of genus $d - d_{x_0} - 1$. Furthermore $\#\widetilde{\mathcal{X}}_{x_0}(\mathbb{F}_q) - \#\mathcal{X}_{x_0}(\mathbb{F}_q)$ equals zero or two. (see Theorem 1). By using the Hasse-Weil bound, we have

$$\left|\#\widetilde{\mathcal{X}}(\mathbb{F}_q) - (q+1)\right| \leq 2(d - d_{x_0} - 1)\sqrt{q}.$$

Then $|\#\mathcal{X}(\mathbb{F}_q) - q| \leq 2(d - d_{x_0} - 1)\sqrt{q} + 1$. Proposition 7 concludes the proof of this proposition.

Theorem 3. *Let $x_0 \in \mathbb{F}_q$. If $x_0 \notin \mathcal{I}$, then*

$$\left|\#\mathtt{Ext}^{-1}(x_0) - q\right| \leq 2(d - d_{x_0} - 1)\sqrt{q} + d_{x_0} + 1.$$

Otherwise,

$$\left|\#\mathtt{Ext}^{-1}(x_0) - q\right| \leq q.$$

Proof. Let $x_0 \in \mathbb{F}_q$. Then Proposition 3 shows that $\#\mathcal{A}_{x_0}(\mathbb{F}_q) = \#\mathtt{Ext}^{-1}(x_0)$. If $x_0 \notin \mathcal{I}$, then Proposition 8 gives the estimate for $\#\mathtt{Ext}^{-1}(x_0)$. If $x_0 \in \mathcal{I}$, then the curve $\mathcal{A}_{x_0}$ is reducible (see Proposition 4). So in this case we have the trivial estimate for $\#\mathtt{Ext}^{-1}(x_0)$.

4.2 Analysis of the Extractor

In this subsection we show that provided the point P is chosen uniformly at random in $\mathcal{C}(\mathbb{F}_{q^2})$, the element extracted from the point P by $\mathtt{Ext}$ is indistinguishable from a uniformly random element in $\mathbb{F}_q$.

Let X be a $\mathbb{F}_q$-valued random variable that is defined as

$$X = \mathtt{Ext}(P), \text{ for } P \in_R \mathcal{C}(\mathbb{F}_{q^2}).$$

Proposition 9. *The random variable X is statistically close to the uniform random variable $U_{\mathbb{F}_q}$.*

$$\Delta(X, U_{\mathbb{F}_q}) = O(\frac{1}{\sqrt{q}}).$$

Proof. Let $z \in \mathbb{F}_q$. For the uniform random variable $U_{\mathbb{F}_q}$, $\Pr[U_{\mathbb{F}_q} = z] = 1/q$. Also for the $\mathbb{F}_q$-valued random variable X,

$$\Pr[X = z] = \frac{\#\mathtt{Ext}^{-1}(z)}{\#\mathcal{C}(\mathbb{F}_{q^2})}.$$

Hasse-Weil's Theorem gives the bound for $\#\mathcal{C}(\mathbb{F}_{q^2})$ and Theorem 3 gives the bound for $\#\mathtt{Ext}^{-1}(z)$. Hence

$$\begin{aligned}\Delta(X,U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\big|\Pr[X=z]-\Pr[U_{\mathbb{F}_q}=z]\big|\\ =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\left|\frac{\#\mathtt{Ext}^{-1}(z)}{\#\mathcal{C}(\mathbb{F}_{q^2})}-\frac{1}{q}\right|\\ =& \sum_{z\in\mathcal{I}}\frac{\big|q\#\mathtt{Ext}^{-1}(z)-\#\mathcal{C}(\mathbb{F}_{q^2})\big|}{2q\#\mathcal{C}(\mathbb{F}_{q^2})}+\sum_{z\in\mathbb{F}_q\setminus\mathcal{I}}\frac{\big|q\#\mathtt{Ext}^{-1}(z)-\#\mathcal{C}(\mathbb{F}_{q^2})\big|}{2q\#\mathcal{C}(\mathbb{F}_{q^2})}.\end{aligned}$$

Let $r=\#\mathcal{I}$. Then

$$\begin{aligned}\Delta(X,U_{\mathbb{F}_q}) \leq& \frac{r(q^2+(d-1)q+1)+(q-r)(2(d-1)q\sqrt{q}+dq+1)}{2q(q^2-(d-1)q+1)}\\ =& \frac{2(d-1)q\sqrt{q}+(d+r)q-2(d-1)r\sqrt{q}-r+1}{2(q^2-(d-1)q+1)}=\frac{d-1+\epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q)=\frac{(d+r)q\sqrt{q}+2(d-1)(d-r-1)q-(r-1)\sqrt{q}-2(d-1)}{2(q^2-(d-1)q+1)}$. If $q\geq 2d^2$, then $\epsilon(q)<1$.

Corollary 1. `Ext` *is a deterministic* $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$*-extractor for* $\mathcal{C}(\mathbb{F}_{q^2})$.

5 Examples

In this section we give some examples for the extractors `Ext`. Our first example is the extractor for the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. For the second example, we recall an extractor in [7] for an elliptic curve defined over $\mathbb{F}_{q^2}$. Also from the result of Theorem 3, we improve the result of [7].

5.1 The Extractor for a Subgroup of $\mathbb{F}_{q^2}^*$

In this subsection we propose a simple extractor for the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. This extractor is the result of Theorem 3, where $f(\mathbf{x})=\mathbf{x}$.

Let G be the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. We recall that every element x in $\mathbb{F}_{q^2}$ is represented in the form $x=x_0\alpha_0+x_1\alpha_1$, where $x_0,x_1\in\mathbb{F}_q$. Define the extractor `ext` for G as the function

$$\begin{aligned}\mathtt{ext}: G &\longrightarrow \mathbb{F}_q\\ \mathtt{ext}(x) &= x_0.\end{aligned}$$

The following proposition gives the estimate for $\#\mathtt{ext}^{-1}(z)$, where $z\in\mathbb{F}_q$.

Proposition 10. *For all* $z\in\mathbb{F}_q^*$,

$$\#\mathtt{ext}^{-1}(z)=\frac{q\pm 1}{2},$$

and for $z=0$, $\#\mathtt{ext}^{-1}(0)=0$ *or* $\#\mathtt{ext}^{-1}(0)=q-1$.

Proof. Let the affine curve $\mathcal{C}$ be defined by the equation $\mathcal{C} : \mathbf{y}^2 = f(\mathbf{x}) = \mathbf{x}$. This curve is of the type considered in Section 4. Clearly for each element $x \in G$, there are exactly two points (x, y) and $(x, -y)$ on $\mathcal{C}$. In fact there is a bijection between G and the set of nonzero abscissa of points on $\mathcal{C}$. Then $\#\mathtt{Ext}^{-1}(z) = 2\#\mathtt{ext}^{-1}(z)$, for all $z \in \mathbb{F}_q^*$. It is easy to see that $\mathcal{I} = \{0\}$. Then Theorem 3 implies the proof of this proposition. Also the bound for $\#\mathtt{ext}^{-1}(0)$ is obvious.

Corollary 2. `ext` *is a deterministic* $(\mathbb{F}_q, \frac{1}{q})$*-extractor for* G*.*

Proof. For $d = 1$, the estimate for $\epsilon(q)$ can be made tighter (see proof of Proposition 9), so that $\epsilon(q) < \frac{1}{q}$.

5.2 The Extractor for Elliptic Curves

In this subsection we recall the extractor introduced by Gürel in [7], that works for an elliptic curve defined over $\mathbb{F}_{q^2}$. This extractor, for a given random point on elliptic curve, outputs the first $\mathbb{F}_q$-coordinate of the abscissa of the point. Then from the result of Theorem 3, we improve the bounds which are proposed in [7].

Let E be an elliptic curve defined over $\mathbb{F}_{q^2}$, where $q = p^k$, for prime number $p > 3$ and positive integer k. Then

$$E(\mathbb{F}_{q^2}) = \{(x, y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} : y^2 = f(x) = x^3 + ax + b\} \cup \{\mathcal{O}_E\},$$

where a and b are in $\mathbb{F}_{q^2}$. Since E is nonsingular, then $f(\mathbf{x})$ is a square free polynomial in $\overline{\mathbb{F}}_q[\mathbf{x}]$.

Let $\alpha_0 = 1$ and $\alpha_1 = t$, where $t \in \mathbb{F}_{q^2}$, such that $t^2 = c$ and c is a non-square element in $\mathbb{F}_q$. So every element x in $\mathbb{F}_{q^2}$ can be represented in the form $x = x_0 + x_1 t$, where $x_0, x_1 \in \mathbb{F}_q$.

The extractor `ext` for E is defined as a function

$$\begin{aligned} \mathtt{ext} : E(\mathbb{F}_{q^2}) &\longrightarrow \mathbb{F}_q \\ \mathtt{ext}(x, y) &= x_0, \\ \mathtt{ext}(\mathcal{O}_E) &= 0. \end{aligned}$$

The following theorem gives the tight bounds for $\#\mathtt{ext}^{-1}(z)$, for all z in $\mathbb{F}_q$.

Proposition 11. *For all* $z \in \mathbb{F}_q^*$*,*

$$\left|\#\mathtt{ext}^{-1}(z) - q\right| \leq 4\sqrt{q} + 1.$$

For $z = 0$*, if* $a_1 \neq 0$ *or* $b_0 \neq 0$*, then*

$$\left|\#\mathtt{ext}^{-1}(0) - (q+1)\right| \leq 4\sqrt{q} + 1,$$

otherwise,

$$\left|\#\mathtt{ext}^{-1}(0) - (q+1)\right| \leq q.$$

Proof. The proof of this theorem follows from Theorems 3, in the case that $f(\mathbf{x}) = \mathbf{x}^3 + a\mathbf{x} + b$. Define the variables $\mathbf{x}_0$ and $\mathbf{x}_1$ by $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1 t$. Then

$$f(\mathbf{x}_0 + \mathbf{x}_1 t) = f_0(\mathbf{x}_0, \mathbf{x}_1) + f_1(\mathbf{x}_0, \mathbf{x}_1)t,$$

where

$$f_0(\mathbf{x}_0, \mathbf{x}_1) = \mathbf{x}_0^3 + 3c\mathbf{x}_0\mathbf{x}_1^2 + a_0\mathbf{x}_0 + ca_1\mathbf{x}_1 + b_0$$
$$f_1(\mathbf{x}_0, \mathbf{x}_1) = c\mathbf{x}_1^3 + 3\mathbf{x}_0^2\mathbf{x}_1 + a_1\mathbf{x}_0 + a_0\mathbf{x}_1 + b_1.$$

Then we fix $\mathbf{x}_0$ by z. It is easy to see that $\mathcal{I} = \{0\}$ if and only if $f_0(z, \mathbf{x}_1) = 0$. Clearly $f_0(z, \mathbf{x}_1) = 0$, if and only if $z = a_1 = b_0 = 0$, since $p \neq 3$. Recall that p is the characteristic of $\mathbb{F}_q$. Also note that $\#\mathtt{ext}^{-1}(0) = \#\mathtt{Ext}^{-1}(0) + 1$, since $\mathtt{ext}(\mathcal{O}_E) = 0$.

Corollary 3. `ext` *is a deterministic* $(\mathbb{F}_q, \frac{3}{\sqrt{q}})$*-extractor for* $E(\mathbb{F}_{q^2})$*, if* $q \geq 18$.

Proof. The proof of this corollary is similar to the proof of Proposition 9, in the case that $d = 3$ and $r \leq 1$.

6 Conclusion

We introduce a deterministic extractor `Ext`, for the (hyper)elliptic curve $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, where q is some power of an odd prime. Our extractor, for a given point P on $\mathcal{C}$, outputs the first $\mathbb{F}_q$-coefficient of the abscissa of the point P. The main part of the analysis of this extractor is to compute $\#\mathtt{Ext}^{-1}(z)$, where $z \in \mathbb{F}_q$. That is equivalent to counting the number of $\mathbb{F}_q$-rational points on the fibers $\mathcal{A}_z$ on the affine variety $\mathcal{A}$. Theorem 3 gives the estimates for $\#\mathtt{Ext}^{-1}(z)$. Our experiments with MAGMA for $\#\mathtt{Ext}^{-1}(z)$, show that the bounds in Theorem 3 are tight. Then we show that if a point P is chosen uniformly at random in $\mathcal{C}$, the element extracted from the point P is statistically close to a uniformly random variable in $\mathbb{F}_q$.

Future Work. Consider the finite field $\mathbb{F}_{q^n}$, where q is a power of a prime p and n is a positive integer. Then $\mathbb{F}_{q^n}$ is a n dimensional vector space over $\mathbb{F}_q$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. That means every element x in $\mathbb{F}_{q^n}$ can be represented in the form $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, where $x_i \in \mathbb{F}_q$.

Let C be an absolutely irreducible nonsingular affine curve that is defined over $\mathbb{F}_{q^n}$ by the equation

$$\mathbf{y}^m = f(\mathbf{x}),$$

where $f(\mathbf{x}) \in \mathbb{F}_{q^n}[\mathbf{x}]$ is a monic square-free polynomial of degree d and m is a positive integer dividing $q - 1$.

We define the extractors $\mathtt{ext}_\ell$ for C, where ℓ is a positive integer less than n. The extractor $\mathtt{ext}_\ell$, for a given point P on the curve, outputs the ℓ *first* $\mathbb{F}_q$-coordinate of the abscissa of the point P.

Definition 11. *Let ℓ be a positive integer less than n. The extractor* $\mathtt{ext}_\ell$ *is defined as a function*

$$\mathtt{ext}_\ell : C(\mathbb{F}_{q^n}) \longrightarrow \mathbb{A}^\ell(\mathbb{F}_q)$$
$$\mathtt{ext}_\ell(x, y) = (x_1, \ldots, x_\ell),$$

where $x \in \mathbb{F}_{q^n}$ is represented as $x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$, for $x_i \in \mathbb{F}_q$.

Let X_ℓ be a $\mathbb{F}_q^\ell$-valued random variable that is defined as

$$X_\ell = \mathtt{ext}_\ell(P), \text{ for } P \in_R C(\mathbb{F}_{q^n}).$$

Conjecture 1. The random variable X_ℓ is $\frac{c}{\sqrt{q^{n-\ell}}}$-uniform on $\mathbb{F}_q^\ell$, where c is a constant depending on m, n and d. That is

$$\Delta(X_\ell, U_{\mathbb{F}_q^\ell}) \leq \frac{c}{\sqrt{q^{n-\ell}}}.$$

We leave the proof of this conjecture for the future work.

Acknowledgment. The authors would like to thank T. Lange for her helpful comments.

References

1. Artin, E.: Algebraic Numbers and Algebraic Functions. Gordon and Breach, New York (1967)
2. Beelen, P., Doumen, J.M.: Pseudorandom sequences from elliptic curves. In: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, pp. 37–52. Springer-Verlag, Berlin Heidelberg (2002)
3. Chevassut, O., Fouque, P., Gaudry, P., Pointcheval, D.: The Twist-Augmented Technique for Key Exchange. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 410–426. Springer, Heidelberg (2006)
4. Cohen, H., Frey, G.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, New York (2006)
5. Farashahi, R.R., Pellikaan, R., Sidorenko, A.: Extractors for Binary Elliptic Curves, Extended Abstract to appear at WCC (2007)
6. Gong, G., Berson, T.A., Stinson, D.R.: Elliptic Curve Pseudorandom Sequence Generators. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 34–48. Springer, Heidelberg (2000)
7. Gürel, N.: Extracting bits from coordinates of a point of an elliptic curve, Cryptology ePrint Archive, Report 2005/324, (2005), `http://eprint.iacr.org/`
8. Hartshorne, R.: Algebraic Geometry, Grad. Texts Math, vol. 52. Springer, Berlin Heidelberg (1977)
9. Hess, F., Shparlinski, I.E.: On the Linear Complexity and Multidimensional Distribution of Congruential Generators over Elliptic Curves. Designs, Codes and Cryptography 35(1), 111–117 (2005)

10. Juels, A., Jakobsson, M., Shriver, E., Hillyer, B.K.: How to turn loaded dice into fair coins. IEEE Transactions on Information Theory 46(3), 911–921 (2000)
11. Kaliski, B.S.: A Pseudo-Random Bit Generator Based on Elliptic Logarithms. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 84–103. Springer, Heidelberg (1987)
12. Lange, T., Shparlinski, I.E.: Certain Exponential Sums and Random Walks on Elliptic Curves. Canad. J. Math. 57(2), 338–350 (2005)
13. —: Distribution of Some Sequences of Points on Elliptic Curves, J. Math. Crypt. 1, 1–11 (2007)
14. Luby, M.: Pseudorandomness and Cryptographic Applications. Princeton University Press, Princeton, USA (1994)
15. Poonen, B.: Bertini Theorems over Finite Fields. Annals of Mathematics 160(3), 1099–1127 (2004)
16. Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. Bulletin of the EATCS 77, 67–95 (2002)
17. Shparlinski, I.E.: On the Naor-Reingold Pseudo-Random Function from Elliptic Curves. Applicable Algebra in Engineering, Communication and Computing—AAECC 11(1), 27–34 (2000)
18. Trevisan, L., Vadhan, S.: Extracting Randomness from Samplable Distributions, IEEE Symposium on Foundations of Computer Science, pp. 32–42 (2000)