Extractors for Binary Elliptic Curves

Reza Rezaeian Farashahi[1,2], Ruud Pellikaan[1], and Andrey Sidorenko[3,⋆]

[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
[3] Brightsight BV Delftechpark 1, 2628 XJ DELFT, The Netherlands

Appeared in: *Designs, Codes and Cryptography*, vol. 49, pp 171–186, 2008

Abstract. We propose a simple and efficient deterministic extractor for an ordinary elliptic curve E, defined over $\mathbb{F}_{2^n}$, where $n = 2\ell$ and ℓ is a positive integer. Our extractor, for a given point P on E, outputs the first $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point P. We also propose a deterministic extractor for the main subgroup G of E, where E has minimal 2-torsion. We show that 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.

Keywords: Elliptic curve, Deterministic extractor, Randomness.

1 Introduction

A deterministic extractor for an elliptic curve is a function that converts a random point on the curve to a bit-string statistically close to uniformly random. In this paper, we propose a simple and efficient deterministic extractor for an ordinary elliptic curve E defined over $\mathbb{F}_{2^n}$, where $n = 2\ell$ and ℓ is an arbitrary positive integer. Our extractor, `ext`, for a given point P on E, outputs the first $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point P. Similarly one could define an extractor that, for a given point P on the curve E, outputs a $\mathbb{F}_{2^\ell}$-linear combination of $\mathbb{F}_{2^\ell}$-coordinates of the abscissa of P. Provided that the point P is chosen uniformly at random in E, the bits extracted from the point P are indistinguishable from a uniformly random bit-string of length ℓ.

The problem of converting random points of an elliptic curve into random bits has several cryptographic applications. One such application is a class of key exchange protocols and key derivation functions 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

⋆ The work was done when the author was a Ph.D. student at TU Eindhoven.

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. Another application of extractors is the design of cryptographically secure pseudorandom generators. An efficient pseudorandom generator based on elliptic curves is proposed by Barker and Kelsey [1]. Unfortunately, their generator (called Dual Elliptic Curve generator) is insecure the reason being that random bits are extracted from random points of the elliptic curve in an improper way [4, 8, 29]. Replacing the extractor used by Barker and Kelsey with one of our extractors yields a pseudorandom generator which is provably secure under the DDH assumption and the x-logarithm assumption [4].

Note that the number of points of any ordinary elliptic curve defined over a finite field with characteristic two is even. Therefore, DDH problem in the corresponding group is easy and thus the group is not suitable for many cryptographic applications. In the case that the order of E equals $2m$ for odd m, we propose a deterministic extractor `Ext` for the subgroup G of order m. In particular, m can be chosen to be prime, so the DDH problem in the subgroup is assumed to be intractable. The extractor `Ext` is a modified version of the extractor `ext`.

Sequences of x-coordinates of pseudorandom points on elliptic curves have been studied in [17, 22, 23, 33]. Kaliski [19] shows that if a point is taken uniformly at random from the union of an elliptic curve and its quadratic twist then the x-coordinate of this point is uniformly distributed in the finite field. 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. [12] and Beelen and Doumen [2] in that they use a function that maps the set of points on an elliptic curve to a set of smaller cardinality. In the former case, this function outputs the trace map of the x-coordinate of the point on a binary curve. So each point gives rise only to one bit. The latter studied more general functions so that some more bits per point can be obtained. Our aim is to extract as many bits as possible while keeping the output distribution statistically close to uniform.

At the moment, several deterministic randomness extractors for elliptic curves are known. One of the extractors is proposed by Gürel [13]. Given a point P on the elliptic curve $\mathrm{E}(\mathbb{F}_{p^2})$ defined over a quadratic extension of a prime field, 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 extracted bits and uniformly random bits is shown to be negligible [13]. Then, Farashahi and Pellikaan [7] define the similar extractor, yet more general, for hyperelliptic curves defined over a quadratic extension of $\mathbb{F}_q$, where q is a power of an odd prime. Furthermore, their result for elliptic curves improve the result of [13]. Another extractor for elliptic curves over prime fields is proposed by Gürel in the same paper. However, the latter extracts essentially less than half of the bits of the

abscissa of P. One more extractor for elliptic curves over prime fields is the TAU technique of Chevassut et al. [5]. 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. Note that both techniques mentioned above can be applied only for elliptic curves over odd prime fields and their extensions, although in many cases elliptic curves over binary fields can be implemented more efficiently in hardware (see, e.g., [14]). Till now, the problem of constructing an efficient deterministic extractor for elliptic curves over binary fields remained open.

2 Preliminaries

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

Notation. Denote by $\mathbb{N}_0$ the set of nonnegative integers and by $\mathbb{R}_0$ the set of nonnegative real numbers. 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 $\mathcal{C}$ be a curve defined over $\mathbb{F}_q$, then the set of $\mathbb{F}_q$-rational points on $\mathcal{C}$ is denoted by $\mathcal{C}(\mathbb{F}_q)$. 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

Let $n = 2\ell$, where ℓ is an arbitrary positive integer. Consider $\mathbb{F}_{2^n}$ as a quadratic extension of $\mathbb{F}_{2^\ell}$. Then $\mathbb{F}_{2^n}$ is a two dimensional vector space over $\mathbb{F}_{2^\ell}$. Let $\{\alpha_1, \alpha_2\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^\ell}$. So every element x in $\mathbb{F}_{2^n}$ can be represented in the form $x = x_1\alpha_1 + x_2\alpha_2$, where x_1 and x_2 are in $\mathbb{F}_{2^\ell}$. We recall that $\{\alpha_1, \alpha_2\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^\ell}$ if and only if

$$\mathcal{D} = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha_1^{2^\ell} & \alpha_2^{2^\ell} \end{vmatrix} \neq 0.$$

Let $\phi : \overline{\mathbb{F}}_{2^\ell} \longrightarrow \overline{\mathbb{F}}_{2^\ell}$ be the Frobenius map defined by $\phi(x) = x^{2^\ell}$. Let

$$\mathrm{Tr} : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^\ell}$$

be the *trace* function. Then $\mathrm{Tr}(x) = x + \phi(x)$, for $x \in \mathbb{F}_{2^n}$. Let

$$\mathrm{N} : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^\ell}$$

be the *norm* function. Then $\mathrm{N}(x) = x\phi(x)$, for $x \in \mathbb{F}_{2^n}$. For more information we refer to [24].

Lemma 1. *Let $x \in \mathbb{F}_{2^n}$. Then $y^2 + y = x$, for some $y \in \mathbb{F}_{2^n}$, if and only if $z^2 + z = \mathrm{Tr}(x)$, for some $z \in \mathbb{F}_{2^\ell}$.*

Proof. Assume $y^2+y = x$, for some $y \in \mathbb{F}_{2^n}$. Let $z = \mathrm{Tr}(y)$. Hence $z^2+z = \mathrm{Tr}(x)$. Now assume that $z^2 + z = \mathrm{Tr}(x)$, for some $z \in \mathbb{F}_{2^\ell}$. Then

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x) = \mathrm{Tr}_{\mathbb{F}_{2^\ell}/\mathbb{F}_2}(\mathrm{Tr}(x)) = \mathrm{Tr}_{\mathbb{F}_{2^\ell}/\mathbb{F}_2}(z^2 + z) = 0.$$

Therefore $x = y^2 + y$, for some $y \in \mathbb{F}_{2^n}$ (see Theorem 2.25 [24]). □

2.2 Binary Elliptic Curve

Let E be an ordinary elliptic curve defined over $\mathbb{F}_{2^n}$. Define the set of $\mathbb{F}_{2^n}$-rational points on E as

$$E(\mathbb{F}_{2^n}) = \{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : y^2 + xy = f(x)\} \cup \{O_E\},$$

where $f(x) = x^3 + ax^2 + b$, such that a and b are in $\mathbb{F}_{2^n}$ and O_E denotes the point at infinity. Note that $b \neq 0$, since the curve is nonsingular.

The reason why we consider ordinary elliptic curves is that solving the discrete logarithm (DL) problem in the group of points of a supersingular elliptic curve is easier than that in a ordinary elliptic curve (see [27]).

2.3 The Newton Polygon and the genus

Definition 1. *Let $\mathbb{F}$ be a field. Let*

$$F(\mathbf{x}, \mathbf{y}) = \sum_{(i,j)\in\mathcal{I}} a_{i,j}\mathbf{x}^i\mathbf{y}^j$$

be a bivariate polynomial, where $\mathcal{I}$ is a finite subset of $\mathbb{N}_0^2$ and $a_{i,j} \in \mathbb{F}^*$ for all $(i, j) \in \mathcal{I}$. Denote by $\Gamma(F)$ the convex hull of the points $(i, j) \in \mathcal{I}$ in $\mathbb{R}_0^2$. The set $\Gamma(F)$ is called the Newton Polygon of F and the boundary of F is denoted by $\partial\Gamma(F)$.

In the following Theorem we recall *Baker's formula* that gives an upper bound for the genus of an irreducible plane curve.

Theorem 1. *Let $\mathcal{C}$ be an irreducible curve defined by the equation $F(\mathbf{x}, \mathbf{y}) = 0$ over an algebraic closed field. Then the genus of the nonsingular model of $\mathcal{C}$ satisfies*

$$g \leq 1 + area\ \Gamma(F) - \tfrac{1}{2}\left\{\partial\Gamma(F) \bigcap \mathbb{N}_0^2\right\}.$$

The right hand side of the above is equal to the number of integral points in the interior of $\Gamma(F)$.

Proof. See [3] or [21]. □

2.4 The Number of Points on a Singular Curve

Let $\mathcal{C}$ be an absolutely irreducible projective plane curve of degree d defined over the finite field $\mathbb{F}_q$.

In case that $\mathcal{C}$ is a nonsingular curve with genus g, then the Hasse-Weil bound gives the following well-known estimate for the number of $\mathbb{F}_q$-rational points on $\mathcal{C}$.

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

The sharper estimate by Serre is

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}\,].$$

In case that $\mathcal{C}$ is a singular curve, denote by $\widetilde{\mathcal{C}}$, the nonsingular projective model of $\mathcal{C}$. Then there is a morphism $\varphi : \widetilde{\mathcal{C}} \longrightarrow \mathcal{C}$, that is a local isomorphism on the nonsingular points on $\mathcal{C}$, and is called the *resolution* or *normalization* of $\mathcal{C}$ (see [9, 15]). If P is a $\mathbb{F}_p$-rational point on $\mathcal{C}$, we define ϑ_P as the number of $\mathbb{F}_p$-rational points on $\widetilde{\mathcal{C}}$, laying over P in the map φ. Then

$$\#\widetilde{\mathcal{C}}(\mathbb{F}_q) - \#\mathcal{C}(\mathbb{F}_q) = \sum_{P \in \mathcal{C}(\mathbb{F}_p)} (\vartheta_P - 1).$$

Let $\mathcal{C}_s(\mathbb{F}_p)$ be the set of singular points of $\mathcal{C}(\mathbb{F}_q)$. Since for a nonsingular points P, we have $\vartheta_P = 1$, then

$$\#\widetilde{\mathcal{C}}(\mathbb{F}_q) - \#\mathcal{C}(\mathbb{F}_q) = \sum_{P \in \mathcal{C}_s(\mathbb{F}_p)} (\vartheta_P - 1).$$

2.5 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 [32, 36].

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*

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

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 [25].

Definition 3. *Let S be a finite set. Let U_k be a random variable uniformly distributed on $\{0,1\}^k$. Consider the function* $\mathrm{Ext} : S \longrightarrow \{0,1\}^k$*. We say that* Ext *is a* δ-deterministic extractor *for S if* $\mathrm{Ext}(U_S)$ *is δ-uniform on $\{0,1\}^k$.*

3 Trace Surface

The elliptic curve E is defined by the equation $\mathbf{y}^2 + \mathbf{xy} = f(\mathbf{x})$. The Artin-Schreier form of E is defined by the equation $\mathbf{y}^2 + \mathbf{y} = g(\mathbf{x})$, where

$$g(\mathbf{x}) = \frac{f(\mathbf{x})}{\mathbf{x}^2} = \mathbf{x} + a + \frac{b}{\mathbf{x}^2}.$$

Let $\overline{\mathbb{F}}_{2^\ell}(\mathbf{x}_1, \mathbf{x}_2)$ be the field of fractions of the polynomial ring $\overline{\mathbb{F}}_{2^\ell}[\mathbf{x}_1, \mathbf{x}_2]$. We extend the Frobenius map ϕ from $\overline{\mathbb{F}}_{2^\ell}$ to $\overline{\mathbb{F}}_{2^\ell}(\mathbf{x}_1, \mathbf{x}_2)$, such that $\phi(\mathbf{x}_i) = \mathbf{x}_i$, for $i = 1, 2$. We define the rational function $\mathcal{F}$ by

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = g(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2) + \phi(g(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2)). \tag{1}$$

Then

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = \mathrm{Tr}(\alpha_1)\mathbf{x}_1 + \mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a) + \frac{\mathcal{D}^2(s_2\mathbf{x}_1 + s_1\mathbf{x}_2)^2}{H^2(\mathbf{x}_1, \mathbf{x}_2)},$$

where

$$\begin{aligned} H(\mathbf{x}_1, \mathbf{x}_2) &= (\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2)\phi(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2) \\ &= \mathrm{N}(\alpha_1)\mathbf{x}_1^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2^2 + \mathcal{D}\mathbf{x}_1\mathbf{x}_2 \end{aligned} \tag{2}$$

and $\sqrt{b} = s_1\alpha_1 + s_2\alpha_2$. Let

$$F(\mathbf{x}_1, \mathbf{x}_2) = (\mathrm{Tr}(\alpha_1)\mathbf{x}_1 + \mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))H^2(\mathbf{x}_1, \mathbf{x}_2) + (\mathcal{D}(s_2\mathbf{x}_1 + s_1\mathbf{x}_2))^2. \tag{3}$$

Definition 4. *Let the affine surface $\mathcal{T}$ over $\mathbb{F}_{2^\ell}$ be defined by the equation*

$$\mathbf{z}^2 + H(\mathbf{x}_1, \mathbf{x}_2)\mathbf{z} = F(\mathbf{x}_1, \mathbf{x}_2).$$

Remark 1. Let $P = (x, y) \in E(\mathbb{F}_{2^n})$, where $x = x_1\alpha_1 + x_2\alpha_2$, $x_1, x_2 \in \mathbb{F}_{2^\ell}$. If $x = 0$, we have $(0, 0, 0) \in \mathcal{T}(\mathbb{F}_{2^\ell})$. Assume $x \neq 0$. So $(\frac{y}{x})^2 + \frac{y}{x} = g(x)$. Let $w = \mathrm{Tr}(\frac{y}{x})$. From equation (1) we have

$$w^2 + w = \mathrm{Tr}(g(x)) = \mathcal{F}(x_1, x_2).$$

Let $z = wN(x) = wH(x_1, x_2)$. Then

$$z^2 + H(x_1, x_2)z = H^2(x_1, x_2)(w^2 + w) = H^2(x_1, x_2)\mathcal{F}(x_1, x_2) = F(x_1, x_2).$$

Hence $(x_1, x_2, z) \in \mathcal{T}(\mathbb{F}_{2^\ell})$.

Lemma 2. *We define the projection map $\pi_E : E(\mathbb{F}_{2^n}) \setminus \{O_E\} \longrightarrow \mathbb{A}^2(\mathbb{F}_{2^\ell})$ by*

$$\pi_E(x, y) = (x_1, x_2),$$

where $x = x_1\alpha_1 + x_2\alpha_2$. Assume that $\pi_E^{-1}(x_1, x_2) \neq \emptyset$. If $x_1 = x_2 = 0$, then $\#\pi_E^{-1}(x_1, x_2) = 1$, otherwise $\#\pi_E^{-1}(x_1, x_2) = 2$.

Proof. Let $P = (x, y) \in \pi_E^{-1}(x_1, x_2)$, where $x = x_1\alpha_1 + x_2\alpha_2$. Clearly $\pi_E^{-1}(0, 0) = \{(0, \sqrt{b})\}$. If $x \neq 0$, then $-P = (x, x + y) \in \pi_E^{-1}(x_0, x_1)$ and $-P \neq P$. Since $P, -P$ are the only points on $E(\mathbb{F}_{2^n})$, with the fixed first coordinate x, then $\pi_E^{-1}(x_0, x_1) = \{P, -P\}$. □

Lemma 3. *We define the projection map* $\pi_{\mathcal{T}} : \mathcal{T}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{A}^2(\mathbb{F}_{2^\ell})$ *by*

$$\pi_{\mathcal{T}}(x_1, x_2, z) = (x_1, x_2).$$

Assume $\pi_{\mathcal{T}}^{-1}(x_1, x_2) \neq \emptyset$. *If* $x_1 = x_2 = 0$, *then* $\#\pi_{\mathcal{T}}^{-1}(x_1, x_2) = 1$, *otherwise* $\#\pi_{\mathcal{T}}^{-1}(x_1, x_2) = 2$.

Proof. Let $(x_1, x_2, z) \in \pi_{\mathcal{T}}^{-1}(x_1, x_2)$. Let $x = x_1\alpha_1 + x_2\alpha_2$. We recall that $H(x_1, x_2) = \mathrm{N}(x)$. So $H(x_1, x_2) = 0$ if and only if $x_1 = x_2 = 0$. Clearly $\pi_{\mathcal{T}}^{-1}(0, 0) = \{(0, 0, 0)\}$. So assume $(x_1, x_2) \neq (0, 0)$. Thus $H(x_1, x_2) \neq 0$. Then (x_1, x_2, z) and $(x_1, x_2, z + H(x_1, x_2))$ are the only points on $\mathcal{T}$, with the first and second coordinates equal x_1 and x_2. Therefore in this case $\pi_{\mathcal{T}}^{-1}(x_1, x_2) = \{(x_1, x_2, z), (x_1, x_2, z + H(x_1, x_2))\}$. □

Proposition 1. *For all* $(x_1, x_2) \in \mathbb{A}^2(\mathbb{F}_q)$,

$$\#\pi_E^{-1}(x_1, x_2) = \#\pi_{\mathcal{T}}^{-1}(x_1, x_2).$$

Proof. First assume that $\pi_E^{-1}(x_1, x_2) \neq \emptyset$. Then there exists a point (x, y) on $E(\mathbb{F}_{2^n})$, such that $x = x_1\alpha_1 + x_2\alpha_2$. If $x = 0$, let $z = 0$, otherwise let $z = \mathrm{Tr}(\frac{y}{x})\mathrm{N}(x)$. Then Remark 1 shows that $(x_1, x_2, z) \in \mathcal{T}(\mathbb{F}_{2^\ell})$. Therefore $(x_1, x_2, z) \in \pi_{\mathcal{T}}^{-1}(x_1, x_2)$ and $\pi_{\mathcal{T}}^{-1}(x_1, x_2) \neq \emptyset$.

Second assume that $\pi_{\mathcal{T}}^{-1}(x_1, x_2) \neq \emptyset$. So there exists a point (x_1, x_2, z) on $\mathcal{T}(\mathbb{F}_q)$. Thus $z^2 + H(x_1, x_2)z = F(x_1, x_2)$. Let $x = x_1\alpha_1 + x_2\alpha_2$. If $x = 0$, let $y = \sqrt{b}$. So $(x, y) \in E(\mathbb{F}_{2^n})$. Now assume $x \neq 0$. Hence $H(x_1, x_2) \neq 0$, since $H(x_1, x_2) = \mathrm{N}(x)$. Let $w = \frac{z}{H(x_1, x_2)}$. From Remark 1 we have, $w^2 + w = \mathrm{Tr}(g(x))$. Lemma 1 implies that there exist $u \in \mathbb{F}_{2^n}$ such that $u^2 + u = g(x)$. Let $y = xu$. Then $(x, y) \in E(\mathbb{F}_{2^n})$. That means $(x, y) \in \pi_E^{-1}(x_1, x_2)$ and $\pi_E^{-1}(x_1, x_2) \neq \emptyset$.

Hence $\pi_E^{-1}(x_1, x_2) \neq \emptyset$ if and only if $\pi_{\mathcal{T}}^{-1}(x_1, x_2) \neq \emptyset$. Furthermore Lemmas 2 and 3 conclude the proof of this proposition. □

Remark 2. In fact, from Proposition 1, one can show that

$$\#E(\mathbb{F}_{2^n}) = \#\mathcal{T}(\mathbb{F}_{2^\ell}) + 1.$$

4 The Extractor for the Elliptic Curve E

In this section we introduce a new extractor for the ordinary elliptic curve E defined over $\mathbb{F}_{2^n}$. This extractor, for a given random point on E, outputs the *first* $\mathbb{F}_{2^\ell}$-coordinate of the abscissa of the point. Then, we show that the output of this extractor, for a given uniformly random point of E, is statistically close to a uniform random variable in $\mathbb{F}_{2^\ell}$.

4.1 The extractor

We recall that $\mathbb{F}_{2^n}$ is the quadratic extension of $\mathbb{F}_{2^\ell}$. So every element x in $\mathbb{F}_{2^n}$ is represented in the form $x = x_1\alpha_1 + x_2\alpha_2$, where x_1 and x_2 are in $\mathbb{F}_{2^\ell}$. In particular $\sqrt{b} = s_1\alpha_1 + s_2\alpha_2$.

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

$$\begin{aligned} \texttt{ext} : E(\mathbb{F}_{2^n}) &\longrightarrow \mathbb{F}_{2^\ell} \\ \texttt{ext}(x, y) &= x_1, \\ \texttt{ext}(O_E) &= 0. \end{aligned}$$

Remark 3. Similarly one could define an extractor that, for a given point P on the curve, outputs a $\mathbb{F}_{2^\ell}$-linear combination of $\mathbb{F}_{2^\ell}$-coordinates of the x-coordinate of P. The analysis of this extractor is exactly the same as our extractor `ext`, since one could interchange the basis $\{\alpha_1, \alpha_2\}$ with a suitable one. So without loss of generality we consider the extractor `ext`.

The following theorem gives tight estimates for $\#\texttt{ext}^{-1}(x_1)$, for all $x_1 \in \mathbb{F}_{2^\ell}$. The result of this theorem is used to analyse the extract `ext`.

Theorem 2. *For all* $x_1 \in \mathbb{F}_{2^\ell}^*$,

$$\left|\#\texttt{ext}^{-1}(x_1) - 2^\ell\right| \leq \begin{cases} [\,4\sqrt{2^\ell}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0, \\ [\,2\sqrt{2^\ell}\,] + 1 & \text{otherwise.} \end{cases}$$

and

$$\left|\#\texttt{ext}^{-1}(0) - (2^\ell + 1)\right| \leq \begin{cases} [\,2\sqrt{2^\ell}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0 \text{ and } s_1 \neq 0, \\ 2^\ell - 1 & \text{if } \mathrm{Tr}(\alpha_2) = s_1 = 0, \\ 1 & \text{otherwise.} \end{cases}$$

For the proof of this theorem we need several propositions and lemmas. Consider the affine variety $\mathcal{T}$ over $\mathbb{F}_{2^\ell}$, by Definition 4. Fix the element x_1 in $\mathbb{F}_{2^\ell}$. Then the points of $\mathcal{T}$ that have the first coordinate equal to x_1 form a curve which we call $\mathcal{T}_{x_1}$.

Let $x_1 \in \mathbb{F}_{2^\ell}$. We define the affine curve $\mathcal{T}_{x_1}$ by the equation

$$T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + H_{x_1}(\mathbf{x}_2)\mathbf{z} + F_{x_1}(\mathbf{x}_2) = 0, \tag{4}$$

where $F_{x_1}(\mathbf{x}_2) = F(x_1, \mathbf{x}_2)$ and $H_{x_1}(\mathbf{x}_2) = H(x_1, \mathbf{x}_2)$.

Proposition 2. *For all* x_1 *in* $\mathbb{F}_{2^\ell}^*$,

$$\#\texttt{ext}^{-1}(x_1) = \#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell})$$

and

$$\#\texttt{ext}^{-1}(0) = 1 + \#\mathcal{T}_0(\mathbb{F}_{2^\ell}).$$

Proof. Let $x_1 \in \mathbb{F}_{2^\ell}^*$. Consider the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{A}}$ from Lemmas 2 and 3. Then

$$\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell}) = \sum_{x_2 \in \mathbb{F}_{2^\ell}} \#\pi_{\mathcal{T}}^{-1}(x_1, x_2)$$

and

$$\#\mathtt{ext}^{-1}(x_1) = \sum_{x_2 \in \mathbb{F}_{2^\ell}} \#\pi_E^{-1}(x_1, x_2).$$

Proposition 1 shows that $\#\pi_E^{-1}(x_1, x_2) = \#\pi_{\mathcal{T}}^{-1}(x_1, x_2)$, for all $x_1, x_2 \in \mathbb{F}_{2^\ell}$. Furthermore $O_E \in \mathtt{ext}^{-1}(0)$. So the proof of this proposition is completed. □

The goal is now to estimate $\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell})$, for all $x_1 \in \mathbb{F}_{2^\ell}$. First we discus this problem for all $x_1 \in \mathbb{F}_{2^\ell}^*$. In Propositions 3 and 4 we show that $\mathcal{T}_{x_1}$ is an absolutely irreducible nonsingular curve, for all $x_1 \in \mathbb{F}_{2^\ell}^*$. Then in Proposition 5 we give the bounds for $\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell})$, for all $x_1 \in \mathbb{F}_{2^\ell}^*$.

Proposition 3. *The affine curve $\mathcal{T}_{x_1}$ is absolutely irreducible, for all $x_1 \in \mathbb{F}_{2^\ell}^*$.*

Proof. The affine curve $\mathcal{T}_{x_1}$, for $x_1 \in \mathbb{F}_{2^\ell}^*$, is defined by the equation (4). So we consider the polynomial

$$T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + H_{x_1}(\mathbf{x}_2)\mathbf{z} + F_{x_1}(\mathbf{x}_2).$$

First suppose $\mathrm{Tr}(\alpha_2) \neq 0$. Then the leading terms of H_{x_1} and F_{x_1} are respectively $\mathrm{N}(\alpha_2)\mathbf{x}_2^2$ and $\mathrm{Tr}(\alpha_2)(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^5$. Hence $\deg(H_{x_1}) = 2$ and $\deg(F_{x_1}) = 5$. Clearly T_{x_1} is absolutely irreducible.

Now suppose $\mathrm{Tr}(\alpha_2) = 0$. Then

$$F_{x_1}(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a))H_{x_1}^2(\mathbf{x}_2) + (\mathcal{D}(s_1\mathbf{x}_2 + s_2x_1))^2.$$

Let

$$R_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + H_{x_1}(\mathbf{x}_2)\mathbf{z} + (\mathcal{D}(s_1\mathbf{x}_2 + s_2x_1))^2.$$

Then T_{x_1} is absolutely irreducible if and only if R_{x_1} is so. Suppose R_{x_1} is reducible. So there exists a bivariate polynomial M in $\overline{\mathbb{F}}_{2^\ell}[\mathbf{x}_2, \mathbf{z}]$, which is a factor of R_{x_1}. We can consider

$$M(\mathbf{x}_2, \mathbf{z}) = \mathbf{z} + m(\mathbf{x}_2) = \mathbf{z} + m_1\mathbf{x}_2 + m_0.$$

We substitute $\mathbf{z}$ by m in the equation of R_{x_1}. Then we have the reminder

$$r(\mathbf{x}_2) = r_3\mathbf{x}_2^3 + r_2\mathbf{x}_2^2 + r_1\mathbf{x}_2 + r_0.$$

Since $r(\mathbf{x}_2) = 0$, so we obtain the following equations.

$$\begin{cases} r_3 = m_1\mathrm{N}(\alpha_2) = 0 \\ r_2 = m_1^2 + \mathcal{D}m_1x_1 + m_0\mathrm{N}(\alpha_2) + (\mathcal{D}s_1)^2 = 0 \\ r_1 = m_1x_1^2\mathrm{N}(\alpha_1) + \mathcal{D}m_0x_1 = 0 \\ r_0 = m_0^2 + m_0x_1^2\mathrm{N}(\alpha_1) + (\mathcal{D}s_2x_1)^2 = 0. \end{cases}$$

Hence $m_1 = 0$. Since $x_1 \neq 0$, so $m_0 = 0$. Then $s_1 = s_2 = 0$. Thus $b = 0$, which is impossible. □

Proposition 4. *The affine curve $\mathcal{T}_{x_1}$ is nonsingular, for all $x_1 \in \mathbb{F}_{2^\ell}^*$.*

Proof. Suppose the affine curve $\mathcal{T}_{x_1}$, for $x_1 \in \mathbb{F}_{2^\ell}^*$, is singular. Then the following system of equations has a solution $(x_2, z) \in \overline{\mathbb{F}}_{2^\ell} \times \overline{\mathbb{F}}_{2^\ell}$.

$$\begin{cases} T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + H_{x_1}(\mathbf{x}_2)\mathbf{z} + F_{x_1}(\mathbf{x}_2) = 0 \\ \dfrac{\partial T_{x_1}}{\partial \mathbf{x}_2}(\mathbf{x}_2, \mathbf{z}) = H'_{x_1}(\mathbf{x}_2)\mathbf{z} + F'_{x_1}(\mathbf{x}_2) = 0 \\ \dfrac{\partial T_{x_1}}{\partial \mathbf{z}}(\mathbf{x}_2, \mathbf{z}) = H_{x_1}(\mathbf{x}_2) = 0, \end{cases} \tag{5}$$

where $H'_{x_1}(\mathbf{x}_2)$ and $F'_{x_1}(\mathbf{x}_2)$ are respectively the derivatives of $H_{x_1}(\mathbf{x}_2)$ and $F_{x_1}(\mathbf{x}_2)$ with respect to $\mathbf{x}_2$. We recall that $H_{x_1}(x_2) = H(x_1, x_2)$ and $F_{x_1}(x_2) = F(x_1, x_2)$. Then from the system (5) and equation (3) we obtain

$$z = \mathcal{D}(s_2 x_1 + s_1 x_2).$$

Because $H'_{x_1}(x_2) = \mathcal{D}x_1$ and $F'_{x_1}(x_2) = 0$, from the second equation we have $\mathcal{D}x_1 z = 0$. Since $x_1 \neq 0$, so $z = 0$. Thus $s_2 x_1 + s_1 x_2 = 0$. Then

$$s_1^2 H(x_1, x_2) = x_1^2 H(s_1, s_2) = x_1^2 \mathrm{N}(\sqrt{b}).$$

Hence $\mathrm{N}(\sqrt{b}) = 0$, since $x_1 \neq 0$. Therefore $b = 0$, which is a contradiction, because E is nonsingular. So the affine curve $\mathcal{T}_{x_1}$ is nonsingular. □

Proposition 5. *For all $x_1 \in \mathbb{F}_{2^\ell}^*$,*

$$\left|\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \begin{cases} [\,4\sqrt{2^\ell}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0, \\ [\,2\sqrt{2^\ell}\,] + 1 & \text{otherwise.} \end{cases}$$

Proof. The affine curve $\mathcal{T}_{x_1}$ is absolutely irreducible and nonsingular by Propositions 3 and 4, for $x_1 \in \mathbb{F}_{2^\ell}^*$. Let $\widetilde{\mathcal{T}}_{x_1}$ be the nonsingular projective model of $\mathcal{T}_{x_1}$.

First suppose $\mathrm{Tr}(\alpha_2) \neq 0$. Then $\widetilde{\mathcal{T}}_{x_1}$ is an imaginary hyperelliptic curve of genus 2. Since $\widetilde{\mathcal{T}}_{x_1}$ has exactly one point at infinity, therefore

$$\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell}) = \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_{2^\ell}) - 1.$$

Now suppose $\mathrm{Tr}(\alpha_2) = 0$. If $\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a) \neq 0$, then $\deg(F_{x_1}) = 4$. By means of the Newton polygon of T_{x_1} we see that the genus of the nonsingular model of $\mathcal{T}_{x_1}$ is at most 1 (see Subsection 2.3). The projective model of $\mathcal{T}_{x_1}$ has only one point at infinity which is a singular point. The number of $\mathbb{F}_{2^\ell}$-rational points on $\widetilde{\mathcal{T}}_{x_1}$, which are lying over the point at infinity in the resolution map, is at most 2 (see subsection 2.4). Hence

$$\left|\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell}) - \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_{2^\ell}) + 1\right| \leq 1.$$

If $\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a) = 0$, then $\deg(F_{x_1}) \leq 2$. The projective model of $\mathcal{T}_{x_1}$ has two points at infinity which are nonsingular points. The genus of the projective model of $\mathcal{T}_{x_1}$ is 1, since the degree of T_{x_1} is 3. Hence

$$\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell}) = \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_{2^\ell}) - 2.$$

By means of Hasse-Weil's Theorem for $\widetilde{\mathcal{T}}_{x_1}$, we obtain the estimates for $\#\mathcal{T}_{x_1}(\mathbb{F}_{2^\ell})$, which concludes the proof of this proposition. □

Now we consider the case that $x_1 = 0$. The curve $\mathcal{T}_0$ is defined by the equation

$$T_0(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2^2\mathbf{z} + F_0(\mathbf{x}_2) = 0,$$

where $F_0(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^4 + (\mathcal{D}s_1\mathbf{x}_2)^2$. Let $\mathbf{w} = \frac{\mathbf{z}}{\mathbf{x}_2}$. By means of this transformation, we define the affine curve $\widehat{\mathcal{T}}_0$ by the equation

$$\widehat{T}_0(\mathbf{x}_2, \mathbf{w}) = \mathbf{w}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2\mathbf{w} + \widehat{F}_0(\mathbf{x}_2) = 0, \tag{6}$$

where $\widehat{F}_0(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^2 + (\mathcal{D}s_1)^2$.

Lemma 4. $\#\widehat{\mathcal{T}}_0(\mathbb{F}_{2^\ell}) = \#\mathcal{T}_0(\mathbb{F}_{2^\ell})$.

Proof. Let $x \in \mathbb{F}_{2^\ell}^*$. It is easy to see that $(x, z) \in \mathcal{T}_0(\mathbb{F}_{2^\ell})$ if and only if $(x, \frac{z}{x}) \in \widehat{\mathcal{T}}_0(\mathbb{F}_{2^\ell})$. Furthermore, the points $(0, 0)$ and $(0, \mathcal{D}s_1)$ are the only points with x-coordinate equals 0 respectively on $\mathcal{T}_0$ and $\widehat{\mathcal{T}}_0$. □

We discuss the irreducibility and nonsingularity of $\widehat{\mathcal{T}}_0$ in Propositions 6 and 7. Then in Proposition 8 we give the bounds for $\#\widehat{\mathcal{T}}_0(\mathbb{F}_{2^\ell})$.

Proposition 6. *The curve $\widehat{\mathcal{T}}_0$ is reducible if and only if* $\mathrm{Tr}(\alpha_2) = s_1 = 0$.

Proof. The affine curve $\widehat{\mathcal{T}}_0$ is defined by the equation (6). If $\mathrm{Tr}(\alpha_2) \neq 0$, then $\deg(\widehat{F}_0) = 3$ and clearly $\widehat{T}_0$ is absolutely irreducible. Now assume $\mathrm{Tr}(\alpha_2) = 0$. Let

$$\widehat{R}_0(\mathbf{x}_2, \mathbf{w}) = \mathbf{w}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2\mathbf{w} + (\mathcal{D}s_1)^2.$$

Then $\widehat{T}_0$ is absolutely irreducible if and only if $\widehat{R}_0$ is so. Furthermore $\widehat{R}_0$ is absolutely irreducible if and only if $s_1 \neq 0$. □

Proposition 7. *The affine curve $\widehat{\mathcal{T}}_0$ is singular if and only if $s_1 = 0$.*

Proof. It is easy to see that the affine curve $\widehat{\mathcal{T}}_0$ has a singular point P if and only if $P = (0, 0)$ and $s_1 = 0$. □

Proposition 8. *The number of $\mathbb{F}_{2^\ell}$-rational points on the affine curve $\widehat{\mathcal{T}}_0$ satisfies*

$$\left|\#\widehat{\mathcal{T}}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \begin{cases} [\,2\sqrt{2^\ell}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0 \text{ and } s_1 \neq 0, \\ 2^\ell - 1 & \text{if } \mathrm{Tr}(\alpha_2) = s_1 = 0, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let $\widetilde{\mathcal{T}_0}$ be the nonsingular projective model of $\widehat{\mathcal{T}_0}$. First suppose $s_1 \neq 0$. From Propositions 6 and 7, the curve $\widehat{\mathcal{T}_0}$ is absolutely irreducible and nonsingular. If $\mathrm{Tr}(\alpha_2) \neq 0$, the curve $\widetilde{\mathcal{T}_0}$ is an elliptic curve. Hence

$$\#\widehat{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) = \#\widetilde{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) - 1.$$

If $\mathrm{Tr}(\alpha_2) = 0$, the curve $\widetilde{\mathcal{T}_0}$ has genus 0. Also it has two points at infinity. So

$$\#\widehat{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) = \#\widetilde{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) - 2.$$

Now suppose $s_1 = 0$. If $\mathrm{Tr}(\alpha_2) \neq 0$, from Proposition 6, the curve $\widehat{\mathcal{T}_0}$ is absolutely irreducible. But it has the singular point $(0, 0)$. Hence the genus of the curve $\widetilde{\mathcal{T}_0}$ equals 0. The number of $\mathbb{F}_{2^\ell}$-rational points on $\widetilde{\mathcal{T}_0}$, which are lying over the point $(0, 0)$ in the resolution map, is 0 or 2. Furthermore the point at infinity is ramified. Hence

$$\#\widehat{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) = \#\widetilde{\mathcal{T}_0}(\mathbb{F}_{2^\ell}) \pm 2.$$

Then, from Hasse-Weil's Theorem for the curve $\widetilde{\mathcal{T}_0}$, we obtain the estimates for $\#\widehat{\mathcal{T}_0}(\mathbb{F}_{2^\ell})$. If $\mathrm{Tr}(\alpha_2) = 0$, from Proposition 6, the curve $\widehat{\mathcal{T}_0}$ is reducible. So we have a trivial bound for $\#\widehat{\mathcal{T}_0}(\mathbb{F}_{2^\ell})$. □

Proof of Theorem 2. Propositions 2 and 5 show the proof of Theorem 2, for $x_1 \in \mathbb{F}_{2^\ell}^*$. Furthermore, Propositions 2, 8 and Lemma 4 show the proof of this theorem, for $x_1 = 0$. □

4.2 Analysis of the Extractor

In this subsection we show that provided the point P is chosen uniformly at random in $E(\mathbb{F}_{2^n})$, the element extracted from the point P by `ext` is indistinguishable from a uniformly random element in $\mathbb{F}_{2^\ell}$.

Let X be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined as

$$X = \mathtt{ext}(P), \text{ for } P \in_R E(\mathbb{F}_{2^n}).$$

Proposition 9. *The random variables X is statistically close to the the uniform random variable $U_{\mathbb{F}_{2^\ell}}$.*

$$\Delta(X, U_{\mathbb{F}_{2^\ell}}) = O(\frac{1}{\sqrt{2^\ell}}).$$

Proof. Let $z \in \mathbb{F}_{2^\ell}$. Then, for the uniform random variable $U_{\mathbb{F}_{2^\ell}}$ in $\mathbb{F}_{2^\ell}$, we have $\Pr[U_{\mathbb{F}_{2^\ell}} = z] = 1/2^\ell$. And for the $\mathbb{F}_{2^\ell}$-valued random variable X,

$$\Pr[X = z] = \frac{\#\mathtt{ext}^{-1}(z)}{\#E(\mathbb{F}_{2^n})}.$$

Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_{2^\ell}}) =& \frac{1}{2} \sum_{z \in \mathbb{F}_{2^\ell}} \left| \Pr[X = z] - \Pr[U_{\mathbb{F}_{2^\ell}} = z] \right| \\ =& \frac{1}{2} \sum_{z \in \mathbb{F}_{2^\ell}} \left| \frac{\#\mathtt{ext}^{-1}(z)}{\#E(\mathbb{F}_{2^n})} - \frac{1}{2^\ell} \right|.\end{aligned}$$

Hasse-Weil's Theorem gives the bound for $\#E(\mathbb{F}_{2^n})$ and Theorem 2 gives the bound for the cardinality of $\mathtt{ext}^{-1}(z)$, for all $z \in \mathbb{F}_{2^\ell}$. Let $g = 2$ if $\mathrm{Tr}(\alpha_2) \neq 0$, otherwise let $g = 1$. In fact g is the maximum genus of curves $\mathcal{T}_{x_1}$, for all $x_1 \in \mathbb{F}_{2^n}$ (see proof of Proposition 5). First assume $s_1 \neq 0$ or $\mathrm{Tr}(\alpha_2) \neq 0$. Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_{2^\ell}}) =& \frac{1}{2^{\ell+1}\#E(\mathbb{F}_{2^n})} \sum_{z \in \mathbb{F}_{2^\ell}} \left| 2^\ell \#\mathtt{ext}^{-1}(z) - \#E(\mathbb{F}_{2^n}) \right| \\ \leq& \frac{2^{\ell+1}\sqrt{2^\ell} g + (4-g)2^\ell - 1}{2(2^\ell - 1)^2} = \frac{g + \epsilon(\ell)}{\sqrt{2^\ell}},\end{aligned}$$

where $\epsilon(\ell) = \frac{(4-g)2^\ell\sqrt{2^\ell} + 2^{\ell+2}g - \sqrt{2^\ell} - 2g}{2(2^\ell-1)^2}$. Indeed $\epsilon(\ell) < 1$, for $\ell \geq 3$.

Now assume $\mathrm{Tr}(\alpha_2) = s_1 = 0$. Theorem 2 gives a trivial bound for $\#\mathtt{ext}^{-1}(0)$. Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_{2^\ell}}) =& \frac{\left| 2^\ell \#\mathtt{ext}^{-1}(0) - \#E(\mathbb{F}_{2^n}) \right|}{2^{\ell+1}\#E(\mathbb{F}_{2^n})} + \sum_{z \in \mathbb{F}^*_{2^\ell}} \frac{\left| 2^\ell \#\mathtt{ext}^{-1}(z) - \#E(\mathbb{F}_{2^n}) \right|}{2^{\ell+1}\#E(\mathbb{F}_{2^n})}. \\ \leq& \frac{(2^{2\ell} + 2^{\ell+1} - 1) + (2^\ell - 1)(2^{\ell+1}\sqrt{2^\ell} + 3 \cdot 2^\ell - 1)}{(2^\ell - 1)^2} \\ =& \frac{2^\ell\sqrt{2^\ell} + 2^{\ell+1} - \sqrt{2^\ell} - 1}{(2^\ell - 1)^2} = \frac{1 + \epsilon(\ell)}{\sqrt{2^\ell}} = \frac{g + \epsilon(\ell)}{\sqrt{2^\ell}},\end{aligned}$$

where $\epsilon(\ell) = \frac{2^{\ell+1}\sqrt{2^\ell} + 2^\ell - \sqrt{2^\ell} - 1}{(2^\ell-1)^2}$. Furthermore $\epsilon(\ell) < 1$, for $\ell \geq 4$. □

Corollary 1. *The extractor* $\mathtt{ext}$ *is an* $\frac{3}{\sqrt{2^\ell}}$*-deterministic for* $E(\mathbb{F}_{2^n})$*, for* $n \geq 8$.

Proof. See proof of Proposition 9. □

5 The Extractor for a Subgroup

In this section we introduce two extractors for the *main subgroup* of the elliptic curve E defined over $\mathbb{F}_{2^n}$, where E has minimal 2-torsion.

Let $\#E(\mathbb{F}_{2^n}) = 2^d m$, where m is odd. If $d = 1$, then E is said to have minimal 2-torsion. Note that E has minimal 2-torsion if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a) = 1$. That means half of the elliptic curves defined over $\mathbb{F}_{2^n}$, have minimal 2-torsion. For more information see [20, 30].

Assume that E has minimal 2-torsion. Hence $\#E(\mathbb{F}_{2^n}) = 2m$. Let G be the subgroup of E of odd order m. E has the point $P_0 = (0, \sqrt{b})$ of order 2. The point

$P = (x, y)$ is in the subgroup G if and only if $P = 2Q$, for some point $Q \in E(\mathbb{F}_{2^n})$. Indeed for the point P in E, $P \in G$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a) = 1$ (see [31, 35]).

Let β be a bit distinguishing $P = (x, y)$ from $-P = (x, x + y)$ satisfying

$$\begin{gathered}\beta : E(\mathbb{F}_{2^n}) \longrightarrow \{0, 1\} \\ \beta(P) = 0, \text{ if } P = -P, \\ \beta(P) + \beta(-P) = 1, \text{ if } P \neq -P.\end{gathered}$$

Note that if $P \in G$ and $P \neq O_E$, then $-P \neq P$, since the order of G is odd. For example the function β can be defined as the least significant bit of y/x, if we consider the polynomial basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Furthermore the point $P = (x, y)$ can be represented by (x, λ), where $\lambda = x+y/x$, is the slope of the doubling. If we represent $P = (x, y)$, by (x, λ), then $-P = (x, x+y)$ is represented by $(x, \lambda+1)$. Hence the function β can be defined as the least significant bit of λ. Another way to define the function β is to define an order on the representation of elements in $\mathbb{F}_{2^n}$. Every element in $\mathbb{F}_{2^n}$ is represented by a bit string. Hence this order, for instance, can be the lexicographical order. Then this order distinguishes y from $x + y$ or P from $-P$.

We define the extractor $\mathtt{Ext}$, as a modified version of the extractor $\mathtt{ext}$ presented in Section 4. Recall that $\mathtt{ext} : E(\mathbb{F}_{2^n}) \longrightarrow \mathbb{F}_{2^\ell}$ is defined by

$$\begin{aligned}\mathtt{ext}(x, y) &= x_1, \\ \mathtt{ext}(O_E) &= 0.\end{aligned}$$

We defined the extractor $\mathtt{Ext}$ as follows.

$$\begin{aligned}\mathtt{Ext} &: G \longrightarrow \mathbb{F}_{2^\ell} \\ \mathtt{Ext}(P) &= \mathtt{ext}(P + \beta(P)P_0).\end{aligned}$$

Let $P = (x, y) \in G$. If $\beta(P) = 0$, then $\mathtt{Ext}(P) = \mathtt{ext}(P)$. If $\beta(P) = 1$, then $\mathtt{Ext}(P) = \mathtt{ext}(P + P_0)$. It is easy to see that the abscissa of the point $P + P_0$ is $\frac{\sqrt{b}}{x}$. Hence

$$\mathtt{Ext}(P) = \begin{cases} x_1, & \text{if } \beta(P) = 0 \\ (\dfrac{\sqrt{b}}{x})_1, & \text{if } \beta(P) = 1. \end{cases}$$

The following proposition gives some bounds for $\#\mathtt{Ext}^{-1}(z)$, for $z \in \mathbb{F}_{2^\ell}$.

Proposition 10. *Let z be a fixed element of $\mathbb{F}_{2^\ell}$. Then*

$$\#\mathtt{ext}^{-1}(z) = 2\#\mathtt{Ext}^{-1}(z).$$

Proof. Define the subset S_z of $\mathtt{ext}^{-1}(z)$ as

$$S_z = \{P \in \mathtt{ext}^{-1}(z) : \beta(P) = 0, \text{ for } P \in G \text{ and } \beta(P + P_0) = 1, \text{ for } P \notin G\}.$$

Let $P \in S_z$. Hence $\texttt{ext}(P) = z$. If $P \in G$, then $\beta(P) = 0$. So $\texttt{Ext}(P) = \texttt{ext}(P) = z$. Thus $P \in \texttt{Ext}^{-1}(z)$. And if $P \notin G$, then $P + P_0 \in G$ and $\beta(P + P_0) = 1$. Hence

$$\texttt{Ext}(P + P_0) = \texttt{ext}(P + P_0 + \beta(P + P_0)P_0) = \texttt{ext}(P) = z.$$

Thus $P + P_0 \in \texttt{Ext}^{-1}(z)$. Let the function $\pi : S_z \longrightarrow \texttt{Ext}^{-1}(z)$ be defined as

$$\pi(P) = \begin{cases} P, & \text{if } P \in G \\ P + P_0, & \text{if } P \notin G \end{cases}$$

It is easy to see that the function π is injective. Let $P \in \texttt{Ext}^{-1}(z)$. Hence $P \in G$ and $\texttt{Ext}(P) = \texttt{ext}(P + \beta(P)P_0) = z$. If $\beta(P) = 0$, then $P \in \texttt{ext}^{-1}(z)$. So $P \in S_z$ and $\pi(P) = P$. If $\beta(P) = 1$, then $P + P_0 \in \texttt{ext}^{-1}(z)$. Since $P + P_0 \notin G$ and $\beta(P) = 1$, then $P + P_0 \in S_z$ and $\pi(P + P_0) = P$. So the function π is surjective and then it is bijective. Therefore $\#S_z = \#\texttt{Ext}^{-1}(z)$.

The points P and $-P$ have the same x-coordinate. So by the definition of $\texttt{ext}$, in section 4, $\texttt{ext}(P) = \texttt{ext}(-P)$. That means $P \in \texttt{ext}^{-1}(z)$ if and only if $-P \in \texttt{ext}^{-1}(z)$. For every pair P and $-P$ in $\texttt{ext}^{-1}(z) \setminus \{O_E, P_0\}$, exactly one of them is in S_z. And in case that $z = 0$, both points O_E and P_0 are in $\texttt{ext}^{-1}(0)$, but only $O_E \in S_z$. Hence $\#\texttt{ext}^{-1}(z) = 2\#S_z$, which concludes the proof of Proposition 10. □

Proposition 11. $\texttt{Ext}$ *is an* $\frac{3}{\sqrt{2^\ell}}$*-deterministic extractor for* G*, for* $n \geq 8$.

Proof. We recall that X is a $\mathbb{F}_{2^\ell}$-valued random variable defined by

$$X = \texttt{ext}(P), \text{ for } P \in_R E(\mathbb{F}_{2^n}).$$

Let X_G be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined by

$$X_G = \texttt{Ext}(P), \text{ for } P \in_R G.$$

Let $z \in \mathbb{F}_{2^\ell}$. Then by Proposition 10 we have

$$\Pr[X_G = z] = \frac{\#\texttt{Ext}^{-1}(z)}{\#G} = \frac{2\#\texttt{Ext}^{-1}(z)}{2\#G} = \frac{\#\texttt{ext}^{-1}(z)}{\#E(\mathbb{F}_{2^n})} = \Pr[X = z].$$

The rest of the proof follows from Corollary 1. □

6 Concluding Remarks

In this section we suggest suitable parameters for the elliptic curves used by our extractors. Also we discuss some implementation issues and open problems.

6.1 Parameters of the Elliptic Curves

The reason why elliptic curves are used in cryptography is that the discrete logarithm (DL) problem in the group of points of an elliptic curve is believed to be intractable for relatively small security parameter. The most efficient methods for solving the DL problem for ordinary elliptic curve have exponential running time. For supersingular elliptic curves there exist subexponential methods, (see [27]) so supersingular elliptic curves should be avoided.

In many cases, it is recommended to use elliptic curves over $\mathbb{F}_{2^n}$, where n is a prime number. Recall that in this paper we consider elliptic curves over $E(\mathbb{F}_{2^n})$, where $n = 2\ell$. To the best of our knowledge, the DL problem for the latter curves is as hard as the one for the former curves provided that the GGHS attack is infeasible, that is, ℓ is a prime number and $\ell \neq 127$ (for more details see [6, 10, 11, 16, 26, 28]).

The finite fields $\mathbb{F}_{2^{178}}, \mathbb{F}_{2^{226}}, \mathbb{F}_{2^{1018}}$ and $\mathbb{F}_{2^{1186}}$ are suggested for elliptic curve cryptography in [6]. For these fields the GGHS attack is infeasible. Furthermore by *ghost bit bases* technique, the arithmetic operations in these fields can be performed more efficiently than in prime extension of $\mathbb{F}_2$ of the same size (see [18, 34]).

The Extractor $\mathtt{Ext}$ is defined in the subgroup G of $E(\mathbb{F}_{2^n})$. For many cryptographic applications m, the order of G, should be prime. Recall that E has minimal 2-torsion. Hence, $\#E(\mathbb{F}_{2^n}) = 2m$.

6.2 Experimental Results

Our experiments with MAGMA for $\#\mathtt{ext}^{-1}(z)$, where $z \in \mathbb{F}_{2^\ell}$, show that the bounds in Theorem 2 are tight.

Also the experiments suggest the following conjecture. Let $E(\mathbb{F}_{2^n})$ be an elliptic curve, where n is a positive integer. In particular n can be prime. Let $P = (x, y) \in E(\mathbb{F}_{2^n})$. Let $x \in \mathbb{F}_{2^n}$ be represented by the bit-string $(x_1, x_2, \ldots, x_n)$. Consider the extractor $\mathtt{ext}$ for $E(\mathbb{F}_{2^n})$ as a function $\mathtt{ext} : E(\mathbb{F}_{2^n}) \longrightarrow \{0,1\}^k$, where $1 \leq k \leq n$, such that the output of $\mathtt{ext}$ for the point P is the k bits of the bit-string of x in fixed positions. For example $\mathtt{ext}$ can be defined as $\mathtt{ext}(P) = (x_1, x_2, \ldots, x_k)$. Let X be a $\{0,1\}^k$-valued random variable that is defined as

$$X = \mathtt{ext}(P), \text{ for } P \in_R E(\mathbb{F}_{2^n}).$$

Conjecture 1. The random variable X is $\frac{g}{\sqrt{2^{n-k}}}$-uniform on $\{0,1\}^k$, where g is constant. That is

$$\Delta(X, U_k) \leq \frac{g}{\sqrt{2^{n-k}}}.$$

We leave the proof of this conjecture as an open problem. Similar to the definition of extractors $\mathtt{Ext}$ in Section 5, one can define an extractor for the main subgroup G of $E(\mathbb{F}_{2^n})$, where E has minimal minimal 2-torsion.

6.3 Conclusion

We introduce a deterministic extractor $\texttt{ext}$ for the ordinary elliptic curve E defined over $\mathbb{F}_{2^n}$, where $n = 2\ell$ and ℓ is a positive integer. The extractor $\texttt{ext}$ for a given point P on E outputs the first $\mathbb{F}_{2^\ell}$-coordinate of the abscissa of P. The main part of the analysis of this extractor is to estimate $\#\texttt{ext}^{-1}(z)$, for all $z \in \mathbb{F}_{2^\ell}$. That is to find the bound for the number of $\mathbb{F}_{2^\ell}$-rational points on the curves $\mathcal{T}_z$ on the trace surface $\mathcal{T}$. Theorem 2 gives tight estimates for $\#\texttt{ext}^{-1}(z)$. By means of the extractor $\texttt{ext}$, we construct the extractor $\texttt{Ext}$ for the main subgroup G of E, where E has minimal 2-torsion. We note that the order of G is odd. In particular if the order of G is prime, then the DDH problem in G is assumed to be intractable, which is crucial for many cryptographic applications. The analysis of the extractor $\texttt{Ext}$ shows that if the point P is chosen uniformly at random in G, then the bits extracted from P are statistically close to a uniformly random bit string of length ℓ.

Acknowledgment. The authors would like to thank T. Lange, B. Schoenmakers and anonymous referees for their helpful comments.

References

1. E. Barker and J. Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, December 2005, NIST Special Publication (SP) 800-90.
2. P. Beelen and J. M. Doumen, *Pseudorandom sequences from elliptic curves*, Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, 2002, pp. 37–52.
3. P. Beelen and R. Pellikaan, *The Newton Polygon of Plane Curves with Many Rational Points*, Designs Codes and Cryptography **21** (2000), 41–67.
4. D. Brown and K. Gjøsteen, *A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator*, Advances in Cryptology–Crypto 2007, Lecture Notes in Computer Science, vol. 4622, Springer, 2007, pp. 466–481.
5. O. Chevassut, P. Fouque, P. Gaudry, and D. Pointcheval, *The Twist-Augmented Technique for Key Exchange*, Public Key Cryptography–PKC 2006, Lecture Notes in Computer Science, vol. 3958, Springer-Verlag, 2006, pp. 410–426.
6. M. Ciet, J. Quisquater, and F. Sica, *A Secure Family of Composite Finite Fields Suitable for Fast Implementation of Elliptic Curve Cryptography*, INDOCRYPT2001, Lecture Notes in Computer Science, vol. 2247, Springer, 2001, pp. 108–116.
7. R. R. Farashahi and R. Pellikaan, *The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic*, International Workshop on the Arithmetic of Finite Fields–WAIFI 2007, Lecture Notes in Computer Science, vol. 4547, Springer-Verlag, 2007, pp. 219–236.
8. R. R. Farashahi, B. Schoenmakers, and A. Sidorenko, *Efficient pseudorandom generators based on the DDH assumption*, Public Key Cryptography–PKC 2007, Lecture Notes in Computer Science, vol. 4450, Springer-Verlag, 2007, pp. 426–441.
9. W. Fulton, *Algebraic Curves : An Introduction to Algebraic Geometry*, Addison-Wesley, 1969.

10. S. Galbraith, F. Hess, and N. P. Smart, *Constructive and Destructive Facets of Weil Descent on Elliptic Curves*, Journal of Cryptology **15** (2002), no. 1, 19–46.
11. ———, *Extending the GHS Weil Descent Attack*, Advances in Cryptology–Eurocrypt , Lecture Notes in Computer Science, vol. 2332, Springer-Verlag, 2002, pp. 29–44.
12. G. Gong, T. A. Berson, and D. R. Stinson, *Elliptic Curve Pseudorandom Sequence Generators*, Selected Areas in Cryptography–SAC 1999, Lecture Notes in Computer Science, vol. 1758, Springer-Verlag, 2000, pp. 34–48.
13. N. Gürel, *Extracting bits from coordinates of a point of an elliptic curve*, Cryptology ePrint Archive, Report 2005/324, 2005, http://eprint.iacr.org/.
14. D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, USA, 2004.
15. R. Hartshorne, *Algebraic Geometry*, Grad. Texts Math, Vol. 52, Springer-Verlag, New York, USA, 1977.
16. F. Hess, *Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm Problem*, LMS Journal of Computation and Mathematics **7** (2004), 167–192.
17. F. Hess and I. E. Shparlinski, *On the Linear Complexity and Multidimensional Distribution of Congruential Generators over Elliptic Curves*, Designs, Codes and Cryptography **35** (2005), no. 1, 111–117.
18. T. Itoh and S. Tsujii, *Structure of Parallel Multipliers for a Class of Fields* $\mathrm{GF}(2^m)$, Informations and Computers **83** (1989), 21–40.
19. B. S. Kaliski, *A Pseudo-Random Bit Generator Based on Elliptic Logarithms*, Advances in Cryptology–Crypto 1986, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 84–103.
20. E. W. Knudsen, *Elliptic Scalar Multiplication Using Point Halving*, Advances in Cryptology–Asiacrypt 1999, Lecture Notes in Computer Science, vol. 1716, Springer-Verlag, 1999, pp. 135–149.
21. A. Kresch, J.L. Wetherell, and M.E. Zieve, *Curves of Every Genus with Many Points, I: Abelian and Toric Families*, J. Algebra **250** (2002), 353–370.
22. T. Lange and I. E. Shparlinski, *Certain Exponential Sums and Random Walks on Elliptic Curves*, Canad. J. Math. **57** (2005), no. 2, 338–350.
23. ———, *Distribution of Some Sequences of Points on Elliptic Curves*, J. Math. Crypt. **1** (2007), 1–11.
24. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Pr., 1994.
25. M. Luby, *Pseudorandomness and Cryptographic Applications*, Princeton University Press, USA, 1994.
26. M. Maurer, A. Menezes, and E. Teske, *Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree*, LMS Journal of Computation and Mathematics **5** (2002), 127–174.
27. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.
28. A. Menezes and E. Teske, *Cryptographic Implications of Hess' Generalized GHS Attack*, Applicable Algebra in Engineering, Communication and Computing—AAECC **16** (2006), no. 6, 439–460.
29. B. Schoenmakers and A. Sidorenko, *Cryptanalysis of the Dual Elliptic Curve pseudorandom generator*, Cryptology ePrint Archive, Report 2006/190, 2006, http://eprint.iacr.org/.
30. R. Schroeppel, *Elliptic curves: Twice as fast!*, 2000, Presentation at the Crypto 2000 Rump Session.

31. G. Seroussi, *Compact Representation of Elliptic Curve Points over* F_{2^n}, Tech. Report HPL-98-94R1, Hewlett–Packard Laboratories, 1998.
32. R. Shaltiel, *Recent Developments in Explicit Constructions of Extractors*, Bulletin of the EATCS **77** (2002), 67–95.
33. I. E. Shparlinski, *On the Naor-Reingold Pseudo-Random Function from Elliptic Curves*, Applicable Algebra in Engineering, Communication and Computing—AAECC **11** (2000), no. 1, 27–34.
34. J. H. Silverman, *Fast Multipication in Finite Fields* $\mathrm{GF}(2^N)$, Cryptographic Hardware and Embedded Systems–CHES 1999, Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, 1999, pp. 122–134.
35. J. A. Solinas, *Efficient Arithmetic on Koblitz Curves*, Designs, Codes and Cryptography **19** (2000), 195–249.
36. L. Trevisan and S. Vadhan, *Extracting Randomness from Samplable Distributions*, IEEE Symposium on Foundations of Computer Science, 2000, pp. 32–42.