Extractors for Binary Elliptic Curves

Reza Rezaeian Farashahi, Ruud Pellikaan, and Andrey Sidorenko
Department of Mathematics and Computing Science,
Eindhoven University of Technology,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
r.rezaeian@tue.nl, g.r.pellikaan@tue.nl, a.sidorenko@tue.nl

December 21, 2006

Abstract

We propose two simple and efficient deterministic extractors for an ordinary elliptic curve E, defined over $\mathbb{F}_{2^N}$, where $N = 2\ell$ and ℓ is a positive integer. Our extractors, for a given point P on E, output respectively the first or the second $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point P. We also propose two deterministic extractors 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.

1 Introduction

A deterministic extractor for an elliptic curve is a function that converts a random point on the curve to a random-looking bit-string, i.e., a bit-string statistically close to uniformly random. In this paper, we propose two simple and efficient deterministic extractors for an ordinary elliptic curve E defined over $\mathbb{F}_{2^N}$, where $N = 2\ell$ and ℓ is an arbitrary positive integer. Our first extractor, $\mathcal{H}_0$, for a given point P on E, outputs the first $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point P. Similarly the second extractor, $\mathcal{H}_1$, for a given point on E, outputs the second $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point. Provided that the point P is chosen uniformly at random in E, the extracted bits of 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 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. Another application of extractors is 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 [21, 8]. 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 [3].

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 two deterministic extractors $\mathtt{Ext}_i$, where $i \in \{0,1\}$, 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. Extractors $\mathtt{Ext}_i$, are modified versions of extractors $\mathcal{H}_i$, $i \in \{0,1\}$. We show that if the point P is chosen uniformly at random in G, the extracted bits of 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 [13, 17, 25]. Kaliski [15] 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 this problem. Our approach is somewhat similar to the basic idea of pseudorandom generators proposed by Gong et al. [9] and Beelen and Doumen [2] in that they use a function that maps the 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 [10]. 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 [10]. In the same paper, Gürel proposes an extractor that is designed for elliptic curves over prime fields. However, the latter extracts essentially less than half of the bits of the abscissa of P. Another extractor for elliptic curves over prime fields is the TAU technique of Chevassut et al. [4]. 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 (see, e.g., [11]). 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. 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 Binary Elliptic Curve

Let E be an ordinary elliptic curve defined over $\mathbb{F}_{2^N}$, that is

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

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.

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 fix the polynomial representation $\mathbb{F}_{2^N} \cong \mathbb{F}_{2^\ell}[t]/(t^2 + t + c)$, where $t^2 + t + c \in \mathbb{F}_{2^\ell}[t]$ is irreducible. Obviously c is a nonzero element of $\mathbb{F}_{2^\ell}$ and $\mathrm{Tr}(c) = 1$, where $\mathrm{Tr} : \mathbb{F}_{2^\ell} \longrightarrow \mathbb{F}_2$ is the trace function. For all x in $\mathbb{F}_{2^N}$, we can write $x = x_0 + x_1 t$, where x_0 and x_1 are in $\mathbb{F}_{2^\ell}$.

2.2 Deterministic Extractor

In our analysis we use the notion of deterministic extractor, so let us recall it briefly. For general definition of extractors we refer to [24, 28].

Definition 2.1. Let S be a finite set. Let U_k be a random variable uniformly distributed on $\{0,1\}^k$. Consider the function $\mathtt{Ext} : S \longrightarrow \{0,1\}^k$. We say that $\mathtt{Ext}$ is a δ-*deterministic extractor* for S if $\mathtt{Ext}(U_S)$ is δ-uniform on $\{0,1\}^k$. That means

$$\Delta(\mathtt{Ext}(U_S), U_k) \leq \delta.$$

3 First Extractor for Binary Elliptic Curves

In this section we introduce a new extractor for the ordinary elliptic curve E defined over $\mathbb{F}_{2^N}$. We recall that $\mathbb{F}_{2^N}$ is the quadratic extension of $\mathbb{F}_{2^\ell}$. The first extractor, for a given random point on E, outputs the *first* $\mathbb{F}_{2^\ell}$-coordinate of the abscissa of the point.

The extractor $\mathcal{H}_0$ is defined as a function

$$\begin{aligned}\mathcal{H}_0 : E(\mathbb{F}_{2^N}) &\longrightarrow \mathbb{F}_{2^\ell}\\ \mathcal{H}_0(x,y) &= x_0,\\ \mathcal{H}_0(O_E) &= 0.\end{aligned}$$

The following theorem gives a tight estimate for $\#\mathcal{H}_0^{-1}(x_0)$, where $x_0 \in \mathbb{F}_{2^\ell}$.

Theorem 3.1. *For all $x_0 \in \mathbb{F}_{2^\ell}^*$,*

$$\left|\#\mathcal{H}_0^{-1}(x_0) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2}\rfloor,$$

and for $x_0 = 0$,

$$\left|\#\mathcal{H}_0^{-1}(0) - (2^\ell+1)\right| \leq \lfloor 2^{(\ell+2)/2}\rfloor.$$

Corollary 3.2. *$\mathcal{H}_0$ is $O(\frac{1}{\sqrt{2^\ell}})$-deterministic extractor for $E(\mathbb{F}_{2^N})$.*

For the proof of Theorem 3.1 we need several propositions and lemmas. Consider the Weil restriction of E to $\mathbb{F}_{2^\ell}$ and fix the element x_0 in $\mathbb{F}_{2^\ell}$. The points of $\mathcal{H}_0^{-1}(x_0)$ form a curve $\mathcal{C}_{x_0}$ in this restriction. The curve $\mathcal{C}_{x_0}$ can be defined by two equations in $\mathbb{A}^3_{\mathbb{F}_{2^\ell}}$ as follows:

$$\begin{cases}\mathcal{F}_0(\mathbf{x}_1,\mathbf{y}_0,\mathbf{y}_1) = c\mathbf{y}_1^2 + c\mathbf{x}_1\mathbf{y}_1 + \mathbf{y}_0^2 + x_0\mathbf{y}_0 + f_0(\mathbf{x}_1) = 0\\ \mathcal{F}_1(\mathbf{x}_1,\mathbf{y}_0,\mathbf{y}_1) = \mathbf{y}_1^2 + (\mathbf{x}_1+x_0)\mathbf{y}_1 + \mathbf{x}_1\mathbf{y}_0 + f_1(\mathbf{x}_1) = 0\end{cases} \tag{3.1}$$

where $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$ are variables and

$$\begin{aligned}f_0(\mathbf{x}_1) &= c\mathbf{x}_1^3 + c(x_0+a_1+a_0)\mathbf{x}_1^2 + x_0^3 + a_0x_0^2 + b_0\\ f_1(\mathbf{x}_1) &= (c+1)\mathbf{x}_1^3 + (x_0+a_1+a_0+ca_1)\mathbf{x}_1^2 + x_0^2\mathbf{x}_1 + a_1x_0^2 + b_1.\end{aligned}$$

Note that $\#\mathcal{H}_0^{-1}(x_0) = \#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell})$, for $x_0 \in \mathbb{F}_{2^\ell}^*$ and $\#\mathcal{H}_0^{-1}(0) = \#\mathcal{C}_0(\mathbb{F}_{2^\ell}) + 1$. The goal is now to compute $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell})$. Let $\mathcal{C}'_{x_0}$ be the plane curve that is defined by the affine equation

$$F_{x_0}(\mathbf{x}_1,\mathbf{y}_0) = \mathrm{Res}_{\mathbf{y}_1}(\mathcal{F}_0,\mathcal{F}_1) = \mathbf{y}_0^4 + g_2(\mathbf{x}_1)\mathbf{y}_0^2 + x_0g_1(\mathbf{x}_1)\mathbf{y}_0 + g_0(\mathbf{x}_1) = 0 \tag{3.2}$$

where

$$\begin{aligned}g_2(\mathbf{x}_1) &= c^2\mathbf{x}_1^2 + cx_0\mathbf{x}_1 + x_0^2 + cx_0^2\\ g_1(\mathbf{x}_1) &= c(c\mathbf{x}_1^2 + x_0\mathbf{x}_1 + x_0^2)\\ g_0(\mathbf{x}_1) &= f_0^2(\mathbf{x}_1) + cx_0(\mathbf{x}_1+x_0)f_0(\mathbf{x}_1) + c^2f_1^2(\mathbf{x}_1) + c^2x_0\mathbf{x}_1f_1(\mathbf{x}_1).\end{aligned}$$

Define the affine curve $\mathcal{A}_{x_0}$ as follows. Let $\mathbf{z}_0 = \mathbf{y}_0(\mathbf{y}_0 + x_0) + c^2\mathbf{x}_1^3$, for $x_0 \in \mathbb{F}_{2^\ell}^*$. Then define the affine curve $\mathcal{A}_{x_0}$ by the equation

$$G_{x_0}(\mathbf{x}_1, \mathbf{z}_0) = \mathbf{z}_0^2 + g_1(\mathbf{x}_1)\mathbf{z}_0 + h_0(\mathbf{x}_1) = 0, \tag{3.3}$$

where $h_0(\mathbf{x}_1) = g_0(\mathbf{x}_1) + c^2\mathbf{x}_1^3 g_1(\mathbf{x}_1) + c^4\mathbf{x}_1^6 = c^4\mathbf{x}_1^5 + \text{l.o.t.}$

If $x_0 = 0$, then

$$\begin{aligned} F_0(\mathbf{x}_1, \mathbf{y}_0) &= \mathbf{y}_0^4 + c^2\mathbf{x}_1^2\mathbf{y}_0^2 + (f_0(\mathbf{x}_1) + cf_1(\mathbf{x}_1))^2 \\ &= (\mathbf{y}_0^2 + c\mathbf{x}_1\mathbf{y}_0 + c^2\mathbf{x}_1^3 + c^2a_1\mathbf{x}_1^2 + b_0 + cb_1)^2 = 0. \end{aligned}$$

For $x_0 = 0$, define the affine curve $\mathcal{A}_0$ to be the reduced curve of $\mathcal{C}_0'$. Hence $\mathcal{A}_0$ is defined by the equation

$$G_0(\mathbf{x}_1, \mathbf{y}_0) = \mathbf{y}_0^2 + c\mathbf{x}_1\mathbf{y}_0 + c^2\mathbf{x}_1^3 + c^2a_1\mathbf{x}_1^2 + b_0 + cb_1 = 0. \tag{3.4}$$

Proposition 3.3. *$\mathcal{A}_{x_0}$ is absolutely irreducible nonsingular affine curve, for all $x_0 \in \mathbb{F}_{2^\ell}^*$.*

Proposition 3.4. *If $x_0 \in \mathbb{F}_{2^\ell}^*$, then*

$$\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2}\rfloor.$$

Proposition 3.5. *The number of $\mathbb{F}_{2^\ell}$-rational points on the affine curve $\mathcal{A}_0$ satisfies*

$$\left|\#\mathcal{A}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2}\rfloor.$$

Proposition 3.6. *The numbers of $\mathbb{F}_{2^\ell}$-rational points on the affine curves $\mathcal{C}_{x_0}$ and $\mathcal{A}_{x_0}$ are equal.*

$$\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}).$$

4 Second Extractor for Binary Elliptic Curve

In this section we introduce another extractor for the ordinary elliptic curve E defined over $\mathbb{F}_{2^N}$. The second extractor, for a given point on the elliptic curve, outputs the *second* $\mathbb{F}_{2^\ell}$-coordinate of the abscissa of the point.

The extractor $\mathcal{H}_1$ is defined as a function

$$\begin{aligned} \mathcal{H}_1 : E(\mathbb{F}_{2^N}) &\longrightarrow \mathbb{F}_{2^\ell} \\ \mathcal{H}_1(x, y) &= x_1, \\ \mathcal{H}_1(O_E) &= 0. \end{aligned}$$

The following theorem gives the estimate for $\#\mathcal{H}_1^{-1}(x_1)$, where x_1 is in $\mathbb{F}_{2^\ell}$.

Theorem 4.1. *For all $x_1 \in \mathbb{F}_{2^\ell}^*$,*

$$\left|\#\mathcal{H}_1^{-1}(x_1) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2}\rfloor + 1.$$

and for $x_1 = 0$, in case that $b_1 \neq 0$, then

$$\left|\#\mathcal{H}_1^{-1}(0) - (2^\ell + 1)\right| \leq 1.$$

and if $x_1 = b_1 = 0$, then

$$\left|\#\mathcal{H}_1^{-1}(0) - (2^\ell + 1)\right| \leq 2^\ell - 1.$$

Corollary 4.2. *$\mathcal{H}_1$ is $O(\frac{1}{\sqrt{2^\ell}})$-deterministic extractor for $E(\mathbb{F}_{2^N})$.*

5 Extractors 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 $\mathrm{Tr}(a) = 1$. That means half of the elliptic curves defined over $\mathbb{F}_{2^N}$, have minimal 2-torsion. If E has minimal 2-torsion, then we can use the point halving technique instead of point doubling. In this method a point $P = (x, y)$ is represented by (x, λ), where $\lambda = x + y/x$ is the slope of the doubling. This representation gives a faster implementation for scalar multiplication based on halving instead of doubling. For more information see [16] and [22].

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 $T = (0, \sqrt{b})$ of order 2. The point $P = (x, y)$ is in the subgroup G if and only if $P = 2Q$ for some point $Q \in E(\mathbb{F}_{2^N})$. That follows assuming $P \in E$, then $P \in G$ if and only if $\mathrm{Tr}(x) = \mathrm{Tr}(a) = 1$. See [23, 27].

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

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

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. We note that the point $P = (x, y)$ can be represented by (x, λ), where $\lambda = x + y/x$. 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.

Let us define the extractors $\mathtt{Ext}_i$, for $i \in \{0, 1\}$. The extractor $\mathcal{H}_i$ in Sections 3 and 4 is defined as the function $\mathcal{H}_i : E(\mathbb{F}_{2^N}) \longrightarrow \mathbb{F}_{2^\ell}$ by

$$\begin{aligned} \mathcal{H}_i(x, y) &= x_i, \\ \mathcal{H}_i(O_E) &= 0. \end{aligned}$$

Define the extractor $\mathtt{Ext}_i$ as follows.

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

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

$$\texttt{Ext}_i(P) = \begin{cases} x_i, & \text{if } \beta(P) = 0 \\ (\frac{\sqrt{b}}{x})_i, & \text{if } \beta(P) = 1. \end{cases}$$

Proposition 5.1. *Let z be a fixed element of $\mathbb{F}_{2^\ell}$. Then*

$$\#\mathcal{H}_i^{-1}(z) = 2\#\texttt{Ext}_i^{-1}(z).$$

Corollary 5.2. $\texttt{Ext}_i$ *is $O(\frac{1}{\sqrt{2^\ell}})$-deterministic extractor for G.*

6 Concluding Remarks

In this section we suggest suitable parameters for the extractors $\texttt{Ext}_i$, where $i \in \{0, 1\}$. Also we discuss some implementational issues.

6.1 Security Parameter

Since the discrete logarithm problem for supersingular curve is rather easier than that for ordinary elliptic curve, then we consider E to be an ordinary elliptic curve. See [19]. Furthermore, for many cryptographic application E is defined over $\mathbb{F}_{2^n}$, where n is a prime number. But it is not so necessary. Recall that we considered E over $E(\mathbb{F}_{2^N})$, where $N = 2\ell$. To make E secure under GGHS attack, let ℓ be a prime number and $\ell \neq 127$. For more details see [5, 6, 7, 12, 18, 20].

The extractors $\texttt{Ext}_i$ are defined in the subgroup G of $E(\mathbb{F}_{2^N})$. For many cryptographic applications m, the order of G, should be prime. We recall that E has minimal 2-torsion. Hence $\#E(\mathbb{F}_{2^N}) = 2m$.

The finite fields $\mathbb{F}_{2^{178}}, \mathbb{F}_{2^{226}}, \mathbb{F}_{2^{1018}}$ and $\mathbb{F}_{2^{1186}}$ are suggested in [5], which are secure under GGHS attack. Furthermore by *ghost bit bases*(GBB) technique (See [26, 14]), the arithmetic operation in these fields can be performed more quickly than in prime extension of $\mathbb{F}_2$ of the same size.

6.2 Experimental Results

Our experiments with MAGMA for $\#\mathcal{H}_i^{-1}(z)$, where $z \in \mathbb{F}_{2^\ell}$, show that the bounds in Theorems 3.1 and 4.1 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 $x \in \mathbb{F}_{2^n}$ is represented by the bit-string $(x_0, x_1, \ldots, x_{n-1})$. Consider the extractor $\texttt{ext}$ for $E(\mathbb{F}_{2^n})$ as a function $\texttt{ext} : E(\mathbb{F}_{2^n}) \longrightarrow \{0, 1\}^k$, where $1 \leq k \leq n$, such that the output of $\texttt{ext}$ for the point $P = (x, y)$ is the k bits of the bit-string of x in fixed positions. For example $\texttt{ext}$ can be defined as

$\mathtt{ext}(P) = (x_0, x_1, \ldots, x_{k-1})$. 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 6.1. The random variable X is statistically close to the the uniform random variable U_k.

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

where g is constant.

We leave the proof of this conjecture as an open problem. Similar to the definition of extractors $\mathtt{Ext}_i$ 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 two deterministic extractors $\mathcal{H}_i$, for the ordinary elliptic curve E defined over $\mathbb{F}_{2^N}$, where $N = 2\ell$ and ℓ is a positive integer. The extractor $\mathcal{H}_0$ (respectively $\mathcal{H}_1$), for a given point P on E outputs the first (respectively the second), $\mathbb{F}_{2^\ell}$-coordinate of the abscissa of P. The main part of the analysis of these extractors is to compute $\#\mathcal{H}_i^{-1}(z)$, for $z \in \mathbb{F}_{2^\ell}$. That is counting the number of $\mathbb{F}_{2^\ell}$-rational points on the fibers $\mathcal{C}_z$ on the Weil restriction $W_{\mathbb{F}_{2^N}/\mathbb{F}_{2^\ell}}(E)$ of E. Theorems 3.1 and 4.1 show tight estimates for $\#\mathcal{H}_i^{-1}(z)$. We use these results to construct two extractors for the main subgroup G of E, where E has minimal 2-torsion. The order of G is odd. In particular if the order of G is prime, then DDH problem in G is assumed to be intractable, which is crucial for many cryptographic applications. The analysis of the extractors 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 and B. Schoenmakers 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] Daniel R. L. Brown, *Conjectured Security of the ANSI-NIST Elliptic Curve RNG*, Cryptology ePrint Archive, Report 2006/117, 2006, `http://eprint.iacr.org/`.

[4] 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.

[5] 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.

[6] 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.

[7] ———, *Extending the GHS Weil Descent Attack*, Advances in Cryptology–Eurocrypt , Lecture Notes in Computer Science, vol. 2332, Springer-Verlag, 2002, pp. 29–44.

[8] Kristian Gjøsteen, *Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005*, March 2006, `http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf`.

[9] G. Gong, T. A. Berson, and D. R. Stinson, *Elliptic Curve Pseudorandom Sequence Generators*, Selected Areas in Cryptography–SAS 1999, Lecture Notes in Computer Science, vol. 1758, Springer-Verlag, 2000, pp. 34–48.

[10] N. Gürel, *Extracting bits from coordinates of a point of an elliptic curve*, Cryptology ePrint Archive, Report 2005/324, 2005, `http://eprint.iacr.org/`.

[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, USA, 2004.

[12] F. Hess, *Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm Problem*, LMS Journal of Computation and Mathematics **7** (2004), 167–192.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] T. Lange and I. E. Shparlinski, *Certain Exponential Sums and Random Walks on Elliptic Curves*, Canad. J. Math. **57** (2005), no. 2, 338–350.

[18] 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.

[19] 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.

[20] 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.

[21] Berry Schoenmakers and Andrey Sidorenko, *Cryptanalysis of the Dual Elliptic Curve pseudorandom generator*, Cryptology ePrint Archive, Report 2006/190, 2006, `http://eprint.iacr.org/`.

[22] R. Schroeppel, *Elliptic curves: Twice as fast!*, 2000, Presentation at the Crypto 2000 Rump Session.

[23] G. Seroussi, *Compact Representation of Elliptic Curve Points over* F_{2^n}, Tech. Report HPL-98-94R1, Hewlett–Packard Laboratories, 1998.

[24] Ronen Shaltiel, *Recent Developments in Explicit Constructions of Extractors*, Bulletin of the EATCS **77** (2002), 67–95.

[25] 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.

[26] J. H. Silverman, *Fast Multipication in Finite Fields* $\mathrm{GF}(2^N)$, Cryptographic Hardware and Embedded Systems–CHES1999, Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, 1999, pp. 122–134.

[27] J. A. Solinas, *Efficient Arithmetic on Koblitz Curves*, Designs, Codes and Cryptography **19** (2000), 195–249.

[28] L. Trevisan and S. Vadhan, *Extracting Randomness from Samplable Distributions*, IEEE Symposium on Foundations of Computer Science, 2000, pp. 32–42.