Extractors for Binary Elliptic Curves

Reza Rezaeian Farashahi
Ruud Pellikaan Andrey Sidorenko

WCC-2007, INRIA Paris, April 19, 2007

Outline

- Introduction
- Preliminaries
- Result
  - Two extractors for a binary elliptic curve
  - Two extractors for a subgroup
  - Proof of the main theorem for the second extractor
- Conclusion

Introduction

- A deterministic extractor for a set is a function that converts a uniformly random point of the set to a bit-string, which is statistically close to a uniformly random bit-string.

- Extractors have several cryptographic applications,
  - Key exchange protocols
  - Key Derivation functions
  - Cryptographically secure pseudo-random generators

Related Works

- Distribution of some sequences of points on curves
  - by Shparlinski, Lange, Hess, Gong, Beelen et al.
- Deterministic extractors for a subgroup of $\mathbb{Z}_p^*$,
  - by Chevassut et al, 2005 and Fouque et al, 2006.
- Deterministic extractors for curves in odd characteristic
  - TAU technique, by Kaliski 1991, and by Chevassut et al, 2005
  - Elliptic curves over $\mathbb{F}_{p^2}$, $\mathbb{F}_p$, by Gürel, 2005
  - (Hyper)elliptic curves over $\mathbb{F}_{q^2}$, by Farashahi et al, 2007
- No efficient extractor for binary elliptic curves has been proposed so far!

Deterministic Extractor

Definition. 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

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

Definition. 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

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

Finite Field $\mathbb{F}_{2^N}$

- $N = 2\ell$, where ℓ is a positive integer.
- Consider $\mathbb{F}_{2^N}$ as a quadratic extension of $\mathbb{F}_{2^\ell}$.
- $\mathbb{F}_{2^N} \cong \mathbb{F}_{2^\ell}[t]/(t^2 + t + c)$, where $t^2 + t + c \in \mathbb{F}_{2^\ell}[t]$ is irreducible.
- For all $x \in \mathbb{F}_{2^N}$, we can write $x = x_0 + x_1 t$, where $x_0, x_1 \in \mathbb{F}_{2^\ell}$.

Binary Elliptic Curve

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

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

where $a, b \in \mathbb{F}_{2^N}$ and $\mathcal{O}_E$ denotes the point at infinity.
Note that $b \neq 0$, since the curve is nonsingular.

New Extractors for E

The extractor $\mathcal{H}_0$:

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

The extractor $\mathcal{H}_1$:

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

Recall that $x = x_0 + x_1 t$.

Analysis of the Extractor $\mathcal{H}_0$

Let X_0 be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined as

$$X_0 = \mathcal{H}_0(P) \text{ for } P \in_R E$$

Proposition. The random variable X_0 is statistically close to the the uniform random variable $U_{\mathbb{F}_{2^\ell}}$.

$$\Delta(X_0, U_{\mathbb{F}_{2^\ell}}) \leq \frac{2 + \epsilon(\ell)}{\sqrt{2^\ell}}.$$

If $\ell \geq 4$ then $\epsilon(\ell) < 1$.

Corollary. The extractor $\mathcal{H}_0$ is a $\frac{3}{\sqrt{2^\ell}}$-*deterministic extractor* for E, for $\ell \geq 4$.

Question: $\#\mathcal{H}_0^{-1}(x_0)$?

Extractors for G, (Setup)

- Let E has minimal 2-torsion, then $\#E(\mathbb{F}_{2^N}) = 2m$, where m is odd.
- Let G be the subgroup of E, which has the odd order m.
- E has the point $T = (0, \sqrt{b})$ of order 2.
- If $P = (x, y) \in E$, then $-P = (x, x + y)$.
- Let β be a bit distinguishing P from $-P$ as follows.

$$\beta : E(\mathbb{F}_{2^N}) \longrightarrow \{0, 1\}$$
$$\text{if } P \in \{\mathcal{O}_E, T\}, \qquad \beta(P) = 0,$$
$$\text{else}, \qquad \beta(P) + \beta(-P) = 1.$$

Extractors for G, (Definition)

The extractor $\mathcal{H}_i$, for $i \in \{0, 1\}$, are defined as $\mathcal{H}_i : E(\mathbb{F}_{2^N}) \longrightarrow \mathbb{F}_{2^\ell}$ by

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

Recall that $x = x_0 + x_1 t$.
Define the extractor $\mathtt{Ext}_i$ as

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

That is :

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

Analysis of the Extractors $\mathtt{Ext}_i$

Proposition. $\#\mathcal{H}_i^{-1}(z) = 2\,\#\mathtt{Ext}_i^{-1}(z)$, for all z in $\mathbb{F}_{2^\ell}$.

Then

Proposition. The extractor $\mathtt{Ext}_0$ is a $\frac{3}{\sqrt{2^\ell}}$-*deterministic extractor* for G, for $\ell \geq 4$.

and

Proposition. The extractor $\mathtt{Ext}_1$ is a $\frac{2}{\sqrt{2^\ell}}$-*deterministic extractor* for G, for $\ell \geq 4$.

Question: $\#\mathcal{H}_i^{-1}(x_i)$?

The Number of Points on E with Fixed x_0

Theorem 1. For all $x_0 \in \mathbb{F}_{2^\ell}^*$,

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

and for $x_0 = 0$,

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

The Number of Points on E with Fixed x_1

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

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

For $x_1 = 0$, if $b_1 \neq 0$, then

$$\#\mathcal{H}_1^{-1}(0) = 2^\ell \pm 1$$

and if $b_1 = 0$, then

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

Outline of the Proof of Theorem 2

- Define the Weil restriction of E, then fix x_1.
- Define the curve $\mathcal{C}_{x_1}$ in this restriction, by two equations with variables $\mathbf{x}_0$, $\mathbf{y}_0$ and $\mathbf{y}_1$.
- Define the curve $\mathcal{C}'_{x_1}$ by the elimination of $\mathbf{y}_0$ in the equations of $\mathcal{C}_{x_1}$.
- Define the curve $\mathcal{A}_{x_1}$ by a transformation from $\mathcal{C}'_{x_1}$.
- Compute $\#\mathcal{A}_{x_1}(\mathbb{F}_{2^\ell})$.
- Show that $\#\mathcal{C}_{x_1}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_1}(\mathbb{F}_{2^\ell})$.

Weil Descent

Let $W_{\mathbb{F}_{2^N}/\mathbb{F}_{2^\ell}}(E)$ be the Weil restriction of $E: \ y^2 + xy = f(x)$
Let $x = \mathbf{x}_0 + \mathbf{x}_1 t$ and $y = \mathbf{y}_0 + \mathbf{y}_1 t$.
Then $E: \ (\mathbf{y}_0 + \mathbf{y}_1 t)^2 + (\mathbf{x}_0 + \mathbf{x}_1 t)(\mathbf{y}_0 + \mathbf{y}_1 t) = f(\mathbf{x}_0 + \mathbf{x}_1 t)$.
After expansion

$$\mathbf{y}_0^2 + c\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_0 + c\mathbf{x}_1\mathbf{y}_1 + (\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + \mathbf{x}_1\mathbf{y}_0 + \mathbf{x}_1\mathbf{y}_1)t = f_0(\mathbf{x}_0, \mathbf{x}_1) + f_1(\mathbf{x}_0, \mathbf{x}_1)t,$$

Hence $W_{\mathbb{F}_{2^N}/\mathbb{F}_{2^\ell}}(E)$ of E is :

$$\begin{cases} \mathbf{y}_0^2 + c\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_0 + c\mathbf{x}_1\mathbf{y}_1 + f_0(\mathbf{x}_0, \mathbf{x}_1) = 0 \\ \mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + \mathbf{x}_1\mathbf{y}_0 + \mathbf{x}_1\mathbf{y}_1 + f_1(\mathbf{x}_0, \mathbf{x}_1) = 0. \end{cases}$$

Note that $W_{\mathbb{F}_{2^N}/\mathbb{F}_{2^\ell}}(E)(\mathbb{F}_{2^\ell}) = E(\mathbb{F}_{2^N})$.

Proof of Theorem 2 (Definition of $\mathcal{C}_{x_1}$)

- Consider the Weil restriction of E to $\mathbb{F}_{2^\ell}$ and fix $x_1 \in \mathbb{F}_{2^\ell}$.
- The points of $\mathcal{H}_1^{-1}(x_1)$ form a curve $\mathcal{C}_{x_1}$ in this restriction as follows.

$$\begin{cases} \mathcal{F}_0(\mathbf{x}_0, \mathbf{y}_0, \mathbf{y}_1) = c\mathbf{y}_1^2 + cx_1\mathbf{y}_1 + \mathbf{y}_0^2 + \mathbf{x}_0\mathbf{y}_0 + f_0(\mathbf{x}_0) = 0 \\ \mathcal{F}_1(\mathbf{x}_0, \mathbf{y}_0, \mathbf{y}_1) = \mathbf{y}_1^2 + (\mathbf{x}_0 + x_1)\mathbf{y}_1 + x_1\mathbf{y}_0 + f_1(\mathbf{x}_0) = 0 \end{cases}$$

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

$$f_0(\mathbf{x}_0) = \mathbf{x}_0^3 + a_0\mathbf{x}_0^2 + cx_1^2\mathbf{x}_0 + cx_1^3 + c(a_1 + a_0)x_1^2 + b_0$$
$$f_1(\mathbf{x}_0) = (x_1 + a_1)\mathbf{x}_0^2 + x_1^2\mathbf{x}_0 + (c+1)x_1^3 + ((c+1)a_1 + a_0)x_1^2 + b_1.$$

- $\#\mathcal{H}_1^{-1}(x_1) = \#\mathcal{C}_{x_1}(\mathbb{F}_{2^\ell})$, for $x_1 \in \mathbb{F}_{2^\ell}^*$ and $\#\mathcal{H}_1^{-1}(0) = \#\mathcal{C}_0(\mathbb{F}_{2^\ell}) + 1$.
- Compute $\#\mathcal{C}_{x_1}(\mathbb{F}_{2^\ell})$.

Proof of Theorem 2 (Definition of $\mathcal{C}'_{x_1}$)

- Let $\mathcal{C}'_{x_1}$ be the plane curve that is defined by the affine equation

$$F_{x_1}(\mathbf{x}_0, \mathbf{y}_1) = \mathrm{Res}_{\mathbf{y}_0}(\mathcal{F}_0, \mathcal{F}_1) = \mathbf{y}_1^4 + g_2(\mathbf{x}_0)\mathbf{y}_1^2 + x_1 g_1(\mathbf{x}_0)\mathbf{y}_1 + g_0(\mathbf{x}_0) = 0$$

where

$$\begin{aligned} g_2(\mathbf{x}_0) &= \mathbf{x}_0^2 + x_1\mathbf{x}_0 + (c+1)x_1^2 \\ g_1(\mathbf{x}_0) &= \mathbf{x}_0^2 + x_1\mathbf{x}_0 + cx_1^2 \\ g_0(\mathbf{x}_0) &= x_1^2 f_0(\mathbf{x}_0) + f_1^2(\mathbf{x}_0) + x_1\mathbf{x}_0 f_1(\mathbf{x}_0) \\ &= (x_1^2 + a_1^2)\mathbf{x}_0^4 + a_1 x_1 \mathbf{x}_0^3 + \text{l.o.t.} \end{aligned}$$

If $x_1 = 0$, then

$$\begin{aligned} F_0(\mathbf{x}_0, \mathbf{y}_1) &= \mathbf{y}_1^4 + \mathbf{x}_0^2\mathbf{y}_1^2 + f_1^2(\mathbf{x}_0) \\ &= (\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + a_1\mathbf{x}_0^2 + b_1)^2 = 0. \end{aligned}$$

Proof of Theorem 2 (Definition of $\mathcal{A}_{x_1}$)

- Define the affine curve $\mathcal{A}_{x_1}$ as follows.
  - For $x_1 \in \mathbb{F}_{2^\ell}^*$, let $\mathbf{z}_1 = \mathbf{y}_1(\mathbf{y}_1 + x_1)$. Then define $\mathcal{A}_{x_1}$, by

$$G_{x_1}(\mathbf{x}_0, \mathbf{z}_1) = \mathbf{z}_1^2 + g_1(\mathbf{x}_0)\mathbf{z}_1 + g_0(\mathbf{x}_0) = 0.$$

  - For $x_1 = 0$, define $\mathcal{A}_0$ by the equation

$$G_0(\mathbf{x}_0, \mathbf{y}_1) = \mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + a_1\mathbf{x}_0^2 + b_1 = 0.$$

Proof of Theorem 2 (Bounds for the cardinality of $\mathcal{A}_{x_1}$)

- If $x_1 \neq 0$, then $\left|\#\mathcal{A}_{x_1}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2\sqrt{2^\ell} \rfloor + 1$
  - The affine curve $\mathcal{A}_{x_1}$ is absolutely irreducible and nonsingular.
  - The projective closure of $\mathcal{A}_{x_1}$, is singular at infinity, if $x_1 \neq a_1$, and nonsingular at infinity if $x_1 = a_1$.
  - The genus of the nonsingular model of of $\mathcal{A}_{x_1}$ is 1.
  - Use Hasse-Weil-Serre bound for the nonsingular model of $\mathcal{A}_{x_1}$.
- If $x_1 = 0$, then
  - If $b_1 \neq 0$, then $\mathcal{A}_0$ is absolutely irreducible and nonsingular of genus 0. Then $\#\mathcal{H}_1^{-1}(0) = 2^\ell \pm 1$.
  - If $b_1 = 0$, then $\mathcal{A}_0$ is reducible. So $2 \leq \#\mathcal{H}_1^{-1}(0) \leq 2^{\ell+1}$.

Proof of Theorem 2 ($\#\mathcal{C}_{x_1} = \#\mathcal{A}_{x_1}$)

- $\#\mathcal{C}_{x_1}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_1}(\mathbb{F}_{2^\ell})$.
  - Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}_{x_1}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{C}}(x_0, y_0, y_1) = x_0$$
  - Define the projection map $\pi_{\mathcal{A}} : \mathcal{A}_{x_1}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{A}}(x_0, z_1) = x_0.$$
  - $\#\pi_{\mathcal{C}}^{-1}(x_0) = \#\pi_{\mathcal{A}}^{-1}(x_0)$, for all $x_0 \in \mathbb{F}_{2^\ell}$.
  - Then
  $$\#\mathcal{C}_{x_1}(\mathbb{F}_{2^\ell}) = \sum_{x_0 \in \mathbb{F}_{2^\ell}} \#\pi_{\mathcal{C}}^{-1}(x_0) = \sum_{x_0 \in \mathbb{F}_{2^\ell}} \#\pi_{\mathcal{A}}^{-1}(x_0) = \#\mathcal{A}_{x_1}(\mathbb{F}_{2^\ell}).$$

Example for the Extractor $\mathtt{Ext}_1$

- Let $\ell = 89$, so $N = 2\ell = 178$.
- $\mathbb{F}_{2^{89}} \cong \mathbb{F}_2[\alpha]/(\alpha^{89} + \alpha^6 + \alpha^5 + \alpha^3 + 1)$.
- $\mathbb{F}_{2^{178}} \cong \mathbb{F}_{2^{89}}[t]/(t^2 + t + 1)$, where $t^2 + t + 1 \in \mathbb{F}_{2^{89}}[t]$ is irreducible.
- $E/\mathbb{F}_{2^{178}} : y^2 + xy = x^3 + ax^2 + b$, where $a = t$, $b = (\alpha^6 + \alpha^4 + \alpha^3 + \alpha) + t$.
- E has minimal 2-torsion, since $\mathrm{Tr}(a) = 1$.
- $\#E = 383123885216472214589586757666800084537735179434295566.$
  $\#E = 2 \times 191561942608236107294793378833400042268867589717147783.$
- G be subgroup E of prime order order m.
  $m = 191561942608236107294793378833400042268867589717147783$.
- $\mathtt{Ext}_1$ is a $\mathbf{2^{-44}}$-deterministic extractor from G.

Summary

- Two extractors $\mathcal{H}_0$ and $\mathcal{H}_1$ for a binary elliptic curve $E/\mathbb{F}_{2^N}$, where N is even.
- Two extractors $\texttt{Ext}_0$ and $\texttt{Ext}_1$ for the subgroup G of E, where $\#E = 2m$ and $\#G = m$, for odd number m.
- Sketch of the proof of Theorem 2 that shows the bounds for $\#\mathcal{H}_1^{-1}(x_1)$.

Thank You!

Questions?