# Extractors for Binary Elliptic Curves

Reza Rezaeian Farashahi Ruud Pellikaan
Andrey Sidorenko

October 11, 2006

# Outline

- Introduction

# Outline

- Introduction
- Preliminaries

# Outline

- Introduction
- Preliminaries
- Result
  - Two extractors for a binary elliptic curve

# Outline

- Introduction
- Preliminaries
- Result
  - Two extractors for a binary elliptic curve
  - Two extractors for a subgroup

# Outline

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

# Outline

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

# Introduction

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

# Introduction

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

# Introduction

- A deterministic extractor for a set is a function that converts a 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
  - Cryptographically secure pseudo-random generators

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

| A | | B |
|---|---|---|
| $a \in_R \mathbb{Z}_q$, $aP$ | $\longrightarrow$ | $aP$ |

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

| A | | B |
|---|---|---|
| $a \in_R \mathbb{Z}_q$, $aP$ | $\longrightarrow$ | $aP$ |
| $bP$ | $\longleftarrow$ | $bP$, $b \in_R \mathbb{Z}_q$ |

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

$$\begin{array}{ccc} \text{A} & & \text{B} \\ a \in_R \mathbb{Z}_q, \ aP & \longrightarrow & aP \\ bP & \longleftarrow & bP, \ b \in_R \mathbb{Z}_q \\ a(bP) & = & b(aP) \end{array}$$

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

$$\begin{array}{ccc} \text{A} & & \text{B} \\ a \in_R \mathbb{Z}_q, \quad aP & \longrightarrow & aP \\ bP & \longleftarrow & bP, \quad b \in_R \mathbb{Z}_q \\ a(bP) & = & b(aP) \end{array}$$

- A and B come up with the common secret $abP$.

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

$$\begin{array}{ccc} & \text{A} & \qquad\qquad \text{B} \\ a \in_R \mathbb{Z}_q, \quad aP & \longrightarrow & aP \\ bP & \longleftarrow & bP, \quad b \in_R \mathbb{Z}_q \\ a(bP) & = & b(aP) \end{array}$$

- A and B come up with the common secret $abP$.
- Decisional Diffie-Hellman assumption, (DDH) for $G$ : $abP$ is indistinguishable from a random element of $G$.

# Diffie-Hellman Key Exchange

- A and B would like to establish a common secret key.
- Let $G$ ba an additive cyclic group of order $q$, with generator $P$.

$$\begin{array}{ccc} & \text{A} & \qquad\qquad \text{B} \\ a \in_R \mathbb{Z}_q, \quad aP & \longrightarrow & aP \\ bP & \longleftarrow & bP, \quad b \in_R \mathbb{Z}_q \\ a(bP) & = & b(aP) \end{array}$$

- A and B come up with the common secret $abP$.
- Decisional Diffie-Hellman assumption, (DDH) for $G$ : $abP$ is indistinguishable from a random element of $G$.
- The goal is to convert $abP$ into random bits.

# Previous Works

- Deterministic extractors for a subgroup of $\mathbb{Z}_p^*$,
  - Subgroup of quadratic residues, where $p = 2q + 1$, and $q$ is also a prime, by O. Chevassut et al, 2005.
  - Subgroup of order $q$, where $q > \sqrt{p}$, by P.-A. Fouque, 2006.

# Previous Works

- Deterministic extractors for a subgroup of $\mathbb{Z}_p^*$,
  - Subgroup of quadratic residues, where $p = 2q + 1$, and $q$ is also a prime, by O. Chevassut et al, 2005.
  - Subgroup of order $q$, where $q > \sqrt{p}$, by P.-A. Fouque, 2006.
- Deterministic extractors for elliptic curves
  - TAU technique, by O. Chevassut et al, 2005
  - Elliptic curves over $\mathbb{F}_{p^2}$, by N. Gürel, 2005
  - Elliptic curves over $\mathbb{F}_p$, by N. Gürel, 2005

# Previous Works

- Deterministic extractors for a subgroup of $\mathbb{Z}_p^*$,
  - Subgroup of quadratic residues, where $p = 2q + 1$, and $q$ is also a prime, by O. Chevassut et al, 2005.
  - Subgroup of order $q$, where $q > \sqrt{p}$, by P.-A. Fouque, 2006.
- Deterministic extractors for elliptic curves
  - TAU technique, by O. Chevassut et al, 2005
  - Elliptic curves over $\mathbb{F}_{p^2}$, by N. Gürel, 2005
  - Elliptic curves over $\mathbb{F}_p$, by N. Gürel, 2005
- No efficient extractor for binary elliptic curves has been proposed so far!

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

- $N = 2\ell$, where $\ell$ is a positive integer.

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

- $N = 2\ell$, where $\ell$ is a positive integer.
- Consider $\mathbb{F}_{2^N}$ as a quadratic extension of $\mathbb{F}_{2^\ell}$.

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

- $N = 2\ell$, where $\ell$ 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.

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

- $N = 2\ell$, where $\ell$ 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.

# Statistical Distance

**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

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

# Statistical Distance

**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

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

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

# Deterministic Extractor

**Definition.** Let $U_k$ be a random variable uniformly distributed on $\{0,1\}^k$. Consider the function

$$\texttt{Ext} : S \longrightarrow \{0,1\}^k.$$

# Deterministic Extractor

**Definition.** Let $U_k$ be a random variable uniformly distributed on $\{0,1\}^k$. Consider the function

$$\texttt{Ext} : S \longrightarrow \{0,1\}^k.$$

We say that $\texttt{Ext}$ is a *$\delta$-deterministic extractor* from $S$ if $\texttt{Ext}(U_S)$ is $\delta$-uniform on $\{0,1\}^k$. That means

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

# New Extractors for $E$

The extractor $\mathcal{H}_0$ :

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

# 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 $\mathcal{H}_1$ :

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

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

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

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

# 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 $U_{\mathbb{F}_{2^\ell}}$.

$$\Delta(X_1, U_{\mathbb{F}_{2^\ell}}) \leq \frac{2 + \epsilon(\ell)}{\sqrt{2^\ell}}.$$

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

# 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 $U_{\mathbb{F}_{2^\ell}}$.

$$\Delta(X_1, U_{\mathbb{F}_{2^\ell}}) \leq \frac{2 + \epsilon(\ell)}{\sqrt{2^\ell}}.$$

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

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

# Analysis of the Extractor $\mathcal{H}_1$

Let $X_1$ be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined as

$$X_1 = \mathcal{H}_1(P) \text{ for } P \in_R E$$

# Analysis of the Extractor $\mathcal{H}_1$

Let $X_1$ be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined as

$$X_1 = \mathcal{H}_1(P) \text{ for } P \in_R E$$

**Proposition.** The random variable $X_1$ is statistically close to the the uniform random variable $U_{\mathbb{F}_{2^\ell}}$.

$$\Delta(X_1, U_{\mathbb{F}_{2^\ell}}) \leq \frac{1+\epsilon(\ell)}{\sqrt{2^\ell}}.$$

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

# Analysis of the Extractor $\mathcal{H}_1$

Let $X_1$ be a $\mathbb{F}_{2^\ell}$-valued random variable that is defined as

$$X_1 = \mathcal{H}_1(P) \text{ for } P \in_R E$$

**Proposition.** The random variable $X_1$ is statistically close to the the uniform random variable $U_{\mathbb{F}_{2^\ell}}$.

$$\Delta(X_1, U_{\mathbb{F}_{2^\ell}}) \leq \frac{1+\epsilon(\ell)}{\sqrt{2^\ell}}.$$

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

**Corollary.** The extractor $\mathcal{H}_1$ is a $\frac{2}{\sqrt{2^\ell}}$-*deterministic extractor* from $E$, for $\ell \geq 4$.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.
- DDH is insecure for $E$.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.
- DDH is insecure for $E$.
- $E$ has the point $T$ of order $2$.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.
- DDH is insecure for $E$.
- $E$ has the point $T$ of order $2$.
- $\#E(\mathbb{F}_{2^N}) = 2^k m$, where $m$ is odd.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.
- DDH is insecure for $E$.
- $E$ has the point $T$ of order $2$.
- $\#E(\mathbb{F}_{2^N}) = 2^k m$, where $m$ is odd.
- Let $G$ be a subgroup of $E$ of order $m$.

# DDH for $E$

- For ordinary elliptic curve $E$, $\#E(\mathbb{F}_{2^N})$ is even.
- DDH is insecure for $E$.
- $E$ has the point $T$ of order $2$.
- $\#E(\mathbb{F}_{2^N}) = 2^k m$, where $m$ is odd.
- Let $G$ be a subgroup of $E$ of order $m$.
- If $m$ is prime, then DDH for $G$ is believed to be intractable.

# Extractors for $G$, (Setup)

- Let $E$ has minimal $2$-torsion, then $\#E(\mathbb{F}_{2^N}) = 2m$, where $m$ is odd.

# 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 $m$.

# 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 $T$ of order $2$.

# 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 $T$ of order $2$.
- If $P = (x, y) \in E$, then $-P = (x, x + y)$.

# 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 $T$ of order $2$.
- If $P = (x, y) \in E$, then $-P = (x, x + y)$.
- Let $\beta$ be a *bit distinguishing* $P$ from $-P$ as follows.

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

# 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

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

# 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

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

Define the extractor $\texttt{Ext}_i$ as

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

# 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

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

Define the extractor $\texttt{Ext}_i$ as

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

That is :

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

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

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

# 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* from $G$, for $\ell \geq 4$.

# 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* from $G$, for $\ell \geq 4$.

and

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

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

- Let $\ell = 89$, so $N = 2\ell = 178$.

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

- Let $\ell = 89$, so $N = 2\ell = 178$.
- $\mathbb{F}_{2^{89}} \cong \mathbb{F}_2[\alpha]/(\alpha^{89} + \alpha^6 + \alpha^5 + \alpha^3 + 1)$.

# 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.

# 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 $a = t$, $b = (\alpha^6 + \alpha^4 + \alpha^3 + \alpha) + t$.

# 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 $\mathrm{Tr}(a) = 1$.

# 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 $\mathrm{Tr}(a) = 1$.
- $\#E = 383123885216472214589586757666800084537735179434295566.$
  $\#E = 2 \times 191561942608236107294793378833400042268867589717147783.$

# 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 $m$.
  $m = 191561942608236107294793378833400042268867589717147783.$

# 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 $2^{-44}$-deterministic extractor from $G$.

# The Number of Points on $E$ with Fixed $x_0$

**Theorem 1.** Let $N_{x_0} = \#\mathcal{H}_0^{-1}(x_0)$, where $x_0$ is in $\mathbb{F}_{2^\ell}$. Then for all $x_0 \in \mathbb{F}_{2^\ell}^*$,

$$\left|N_{x_0} - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor,$$

# The Number of Points on $E$ with Fixed $x_0$

**Theorem 1.** Let $N_{x_0} = \#\mathcal{H}_0^{-1}(x_0)$, where $x_0$ is in $\mathbb{F}_{2^\ell}$. Then for all $x_0 \in \mathbb{F}_{2^\ell}^*$,

$$\left|N_{x_0} - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor,$$

and for $x_0 = 0$,

$$\left|N_0 - (2^\ell + 1)\right| \leq \lfloor 2^{(\ell+2)/2} \rfloor.$$

# The Number of Points on $E$ with Fixed $x_1$

**Theorem 2.** Let $N_{x_1} = \#\mathcal{H}_1^{-1}(x_1)$, where $x_1$ is in $\mathbb{F}_{2^\ell}$. Then for all $x_1 \in \mathbb{F}_{2^\ell}^*$,

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

# The Number of Points on $E$ with Fixed $x_1$

**Theorem 2.** Let $N_{x_1} = \#\mathcal{H}_1^{-1}(x_1)$, where $x_1$ is in $\mathbb{F}_{2^\ell}$. Then for all $x_1 \in \mathbb{F}_{2^\ell}^*$,

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

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

$$\left|N_0 - (2^\ell + 1)\right| \leq 1.$$

# The Number of Points on $E$ with Fixed $x_1$

**Theorem 2.** Let $N_{x_1} = \#\mathcal{H}_1^{-1}(x_1)$, where $x_1$ is in $\mathbb{F}_{2^\ell}$. Then for all $x_1 \in \mathbb{F}_{2^\ell}^*$,

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

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

$$\left|N_0 - (2^\ell + 1)\right| \leq 1.$$

and if $x_1 = b_1 = 0$, then

$$\left|N_0 - (2^\ell + 1)\right| \leq 2^\ell - 1.$$

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.
- Define the curve $\mathcal{C}_{x_0}$ in this restriction, by two equations and variables $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$.

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.
- Define the curve $\mathcal{C}_{x_0}$ in this restriction, by two equations and variables $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$.
- Define the curve $\mathcal{C}'_{x_0}$ by the elimination of $\mathbf{y}_1$ in the equations of $\mathcal{C}_{x_0}$.

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.
- Define the curve $\mathcal{C}_{x_0}$ in this restriction, by two equations and variables $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$.
- Define the curve $\mathcal{C}'_{x_0}$ by the elimination of $\mathbf{y}_1$ in the equations of $\mathcal{C}_{x_0}$.
- Define the curve $\mathcal{A}_{x_0}$ by a transformation from $\mathcal{C}'_{x_0}$.

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.
- Define the curve $\mathcal{C}_{x_0}$ in this restriction, by two equations and variables $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$.
- Define the curve $\mathcal{C}'_{x_0}$ by the elimination of $\mathbf{y}_1$ in the equations of $\mathcal{C}_{x_0}$.
- Define the curve $\mathcal{A}_{x_0}$ by a transformation from $\mathcal{C}'_{x_0}$.
- Compute $\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.

# Outline of the Proof of Theorem 1

- Define the Weil restriction of $E$, then fix $x_0$.
- Define the curve $\mathcal{C}_{x_0}$ in this restriction, by two equations and variables $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$.
- Define the curve $\mathcal{C}'_{x_0}$ by the elimination of $\mathbf{y}_1$ in the equations of $\mathcal{C}_{x_0}$.
- Define the curve $\mathcal{A}_{x_0}$ by a transformation from $\mathcal{C}'_{x_0}$.
- Compute $\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.
- Show that $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.

# Weil Decent

Let $W_{\mathbb{F}_{2^N}/\mathbb{F}_{2^\ell}}(E)$ be the Weil restriction of $E: \ y^2 + xy = f(x)$

# Weil Decent

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 $y = \mathbf{y}_0 + \mathbf{y}_1 t$.

# Weil Decent

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 $E: \ (\mathbf{y}_0 + \mathbf{y}_1 t)^2 + (\mathbf{x}_0 + \mathbf{x}_1 t)(\mathbf{y}_0 + \mathbf{y}_1 t) = f(\mathbf{x}_0 + \mathbf{x}_1 t).$

# Weil Decent

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

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

# Weil Decent

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 :

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

# Weil Decent

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 1 ( Definition of $\mathcal{C}_{x_0}$)

- Consider the Weil restriction of $E$ to $\mathbb{F}_{2^\ell}$ and fix $x_0 \in \mathbb{F}_{2^\ell}$.

# Proof of Theorem 1 ( Definition of $\mathcal{C}_{x_0}$)

- Consider the Weil restriction of $E$ to $\mathbb{F}_{2^\ell}$ and fix $x_0 \in \mathbb{F}_{2^\ell}$.
- The points of $\mathcal{H}_0^{-1}(x_0)$ form a curve $\mathcal{C}_{x_0}$ in this restriction as follows.

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

# Proof of Theorem 1 ( Definition of $\mathcal{C}_{x_0}$)

- Consider the Weil restriction of $E$ to $\mathbb{F}_{2^\ell}$ and fix $x_0 \in \mathbb{F}_{2^\ell}$.
- The points of $\mathcal{H}_0^{-1}(x_0)$ form a curve $\mathcal{C}_{x_0}$ in this restriction as follows.

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

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

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

# Proof of Theorem 1 ( Definition of $\mathcal{C}_{x_0}$)

- Consider the Weil restriction of $E$ to $\mathbb{F}_{2^\ell}$ and fix $x_0 \in \mathbb{F}_{2^\ell}$.
- The points of $\mathcal{H}_0^{-1}(x_0)$ form a curve $\mathcal{C}_{x_0}$ in this restriction as follows.

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

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

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

- $N_{x_0} = \#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell})$, for $x_0 \in \mathbb{F}_{2^\ell}^*$ and $N_0 = \#\mathcal{C}_0(\mathbb{F}_{2^\ell}) + 1$.

# Proof of Theorem 1 ( Definition of $\mathcal{C}_{x_0}$)

- Consider the Weil restriction of $E$ to $\mathbb{F}_{2^\ell}$ and fix $x_0 \in \mathbb{F}_{2^\ell}$.
- The points of $\mathcal{H}_0^{-1}(x_0)$ form a curve $\mathcal{C}_{x_0}$ in this restriction as follows.

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

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

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

- $N_{x_0} = \#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell})$, for $x_0 \in \mathbb{F}_{2^\ell}^*$ and $N_0 = \#\mathcal{C}_0(\mathbb{F}_{2^\ell}) + 1$.
- Compute $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell})$

# Proof of Theorem 1 (Definition of $\mathcal{C}'_{x_0}$)

- Let $\mathcal{C}'_{x_0}$ be the plane curve that is defined by the affine equation

$$F_{x_0}(\mathbf{x}_1, \mathbf{y}_0) = \mathrm{Res}_{\mathbf{y}_1}(\mathcal{F}_0, \mathcal{F}_1) = \mathbf{y}_0^4 + g_2(\mathbf{x}_1)\mathbf{y}_0^2 + x_0 g_1(\mathbf{x}_1)\mathbf{y}_0 + g_0(\mathbf{x}_1) = 0$$

# Proof of Theorem 1 (Definition of $\mathcal{C}'_{x_0}$)

- Let $\mathcal{C}'_{x_0}$ be the plane curve that is defined by the affine equation

$$F_{x_0}(\mathbf{x}_1, \mathbf{y}_0) = \mathrm{Res}_{\mathbf{y}_1}(\mathcal{F}_0, \mathcal{F}_1) = \mathbf{y}_0^4 + g_2(\mathbf{x}_1)\mathbf{y}_0^2 + x_0 g_1(\mathbf{x}_1)\mathbf{y}_0 + g_0(\mathbf{x}_1) = 0$$

where

$$\begin{aligned} g_2(\mathbf{x}_1) &= c^2\mathbf{x}_1^2 + cx_0\mathbf{x}_1 + x_0^2 + cx_0^2 \\ g_1(\mathbf{x}_1) &= c(c\mathbf{x}_1^2 + x_0\mathbf{x}_1 + x_0^2) \\ g_0(\mathbf{x}_1) &= f_1^2(\mathbf{x}_1) + cx_0(\mathbf{x}_1 + x_0)f_0(\mathbf{x}_1) + c^2 f_2^2(\mathbf{x}_1) + c^2 x_0 \mathbf{x}_1 f_1(\mathbf{x}_1) \\ &= c^4\mathbf{x}_1^6 + c^3(x_0 + ca_1^2)\mathbf{x}_1^4 + \text{l.o.t.} \end{aligned}$$

# Proof of Theorem 1 (Definition of $\mathcal{C}'_{x_0}$)

- Let $\mathcal{C}'_{x_0}$ be the plane curve that is defined by the affine equation

$$F_{x_0}(\mathbf{x}_1, \mathbf{y}_0) = \mathrm{Res}_{\mathbf{y}_1}(\mathcal{F}_0, \mathcal{F}_1) = \mathbf{y}_0^4 + g_2(\mathbf{x}_1)\mathbf{y}_0^2 + x_0 g_1(\mathbf{x}_1)\mathbf{y}_0 + g_0(\mathbf{x}_1) = 0$$

where

$$\begin{aligned} g_2(\mathbf{x}_1) &= c^2\mathbf{x}_1^2 + cx_0\mathbf{x}_1 + x_0^2 + cx_0^2 \\ g_1(\mathbf{x}_1) &= c(c\mathbf{x}_1^2 + x_0\mathbf{x}_1 + x_0^2) \\ g_0(\mathbf{x}_1) &= f_1^2(\mathbf{x}_1) + cx_0(\mathbf{x}_1 + x_0)f_0(\mathbf{x}_1) + c^2 f_2^2(\mathbf{x}_1) + c^2 x_0 \mathbf{x}_1 f_1(\mathbf{x}_1) \\ &= c^4\mathbf{x}_1^6 + c^3(x_0 + ca_1^2)\mathbf{x}_1^4 + \text{l.o.t.} \end{aligned}$$

If $x_0 = 0$, then

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

# Proof of Theorem 1 ( Definition of $\mathcal{A}_{x_0}$)

- Define the affine curve $\mathcal{A}_{x_0}$ as follows.

# Proof of Theorem 1 ( Definition of $\mathcal{A}_{x_0}$)

- Define the affine curve $\mathcal{A}_{x_0}$ as follows.
  - For $x_0 \in \mathbb{F}_{2^\ell}^*$, let $\mathbf{z}_0 = \mathbf{y}_0(\mathbf{y}_0 + x_0)$. Then define $\mathcal{A}_{x_0}$, by

$$G_{x_0}(\mathbf{x}_1, \mathbf{z}_0) = \mathbf{z}_0^2 + g_1(\mathbf{x}_1)\mathbf{z}_0 + g_0(\mathbf{x}_1) = 0.$$

# Proof of Theorem 1 ( Definition of $\mathcal{A}_{x_0}$)

- Define the affine curve $\mathcal{A}_{x_0}$ as follows.
  - For $x_0 \in \mathbb{F}_{2^\ell}^*$, let $\mathbf{z}_0 = \mathbf{y}_0(\mathbf{y}_0 + x_0)$. Then define $\mathcal{A}_{x_0}$, by

$$G_{x_0}(\mathbf{x}_1, \mathbf{z}_0) = \mathbf{z}_0^2 + g_1(\mathbf{x}_1)\mathbf{z}_0 + g_0(\mathbf{x}_1) = 0.$$

  - For $x_0 = 0$, define $\mathcal{A}_0$ by the equation

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

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_{x_0}$.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_{x_0}$.
- If $x_0 = 0$, then $\left|\#\mathcal{A}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2} \rfloor$.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_{x_0}$.
- If $x_0 = 0$, then $\left|\#\mathcal{A}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2} \rfloor$.
  - If $b_0 + cb_1 \neq 0$, then $\mathcal{A}_0$ is an elliptic curve.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_{x_0}$.
- If $x_0 = 0$, then $\left|\#\mathcal{A}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2} \rfloor$.
  - If $b_0 + cb_1 \neq 0$, then $\mathcal{A}_0$ is an elliptic curve.
  - If $b_0 + cb_1 = 0$, then $\mathcal{A}_0$ is singular and the genus of $\widetilde{\mathcal{A}}_0$ is $0$.

# Proof of Theorem 1 ($\#\mathcal{A}_{x_0}$)

- If $x_0 \neq 0$, then $\left|\#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq 2\lfloor 2^{(\ell+2)/2} \rfloor$.
  - The affine curve $\mathcal{A}_{x_0}$ is absolutely irreducible.
  - The affine curve $\mathcal{A}_{x_0}$ is nonsingular.
  - The projective closure of $\mathcal{A}_{x_0}$, is singular at infinity.
  - From the Newton polygon of $G_{x_0}$, the genus of $\widetilde{\mathcal{A}}_{x_0}$ is at most $2$, where $\widetilde{\mathcal{A}}_{x_0}$ is the nonsingular model of $\mathcal{A}_{x_0}$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_{x_0}$.
- If $x_0 = 0$, then $\left|\#\mathcal{A}_0(\mathbb{F}_{2^\ell}) - 2^\ell\right| \leq \lfloor 2^{(\ell+2)/2} \rfloor$.
  - If $b_0 + cb_1 \neq 0$, then $\mathcal{A}_0$ is an elliptic curve.
  - If $b_0 + cb_1 = 0$, then $\mathcal{A}_0$ is singular and the genus of $\widetilde{\mathcal{A}}_0$ is $0$.
  - Use Hasse-Weil or Serre bound for $\widetilde{\mathcal{A}}_0$.

# Proof of Theorem 1 ($\#\mathcal{C}_{x_0} = \#\mathcal{A}_{x_0}$)

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

# Proof of Theorem 1 ($\#\mathcal{C}_{x_0} = \#\mathcal{A}_{x_0}$)

- $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.
  - Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by

$$\pi_{\mathcal{C}}(x_1, y_0, y_1) = x_1$$

# Proof of Theorem 1 ($\#\mathcal{C}_{x_0} = \#\mathcal{A}_{x_0}$)

- $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.
  - Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by

$$\pi_{\mathcal{C}}(x_1, y_0, y_1) = x_1$$

  - Define the projection map $\pi_{\mathcal{A}} : \mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by

$$\pi_{\mathcal{A}}(x_1, z_0) = x_1.$$

# Proof of Theorem 1 ($\#\mathcal{C}_{x_0} = \#\mathcal{A}_{x_0}$)

- $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.
  - Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{C}}(x_1, y_0, y_1) = x_1$$
  - Define the projection map $\pi_{\mathcal{A}} : \mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{A}}(x_1, z_0) = x_1.$$
  - $\#\pi_{\mathcal{C}}^{-1}(x_1) = \#\pi_{\mathcal{A}}^{-1}(x_1)$, for all $x_1 \in \mathbb{F}_{2^\ell}$.

# Proof of Theorem 1 ($\#\mathcal{C}_{x_0} = \#\mathcal{A}_{x_0}$)

- $\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell})$.
  - Define the projection map $\pi_{\mathcal{C}} : \mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{C}}(x_1, y_0, y_1) = x_1$$
  - Define the projection map $\pi_{\mathcal{A}} : \mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}) \longrightarrow \mathbb{F}_{2^\ell}$, by
  $$\pi_{\mathcal{A}}(x_1, z_0) = x_1.$$
  - $\#\pi_{\mathcal{C}}^{-1}(x_1) = \#\pi_{\mathcal{A}}^{-1}(x_1)$, for all $x_1 \in \mathbb{F}_{2^\ell}$.
  - Then
  $$\#\mathcal{C}_{x_0}(\mathbb{F}_{2^\ell}) = \sum_{x_1 \in \mathbb{F}_{2^\ell}} \#\pi_{\mathcal{C}}^{-1}(x_1) = \sum_{x_1 \in \mathbb{F}_{2^\ell}} \#\pi_{\mathcal{A}}^{-1}(x_1) = \#\mathcal{A}_{x_0}(\mathbb{F}_{2^\ell}).$$

# Summary

- Two extractors $\mathcal{H}_0$ and $\mathcal{H}_1$ for a binary elliptic curve $E/\mathbb{F}_{2^N}$, where $N$ is even.

# 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 $m$.

# 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 1 that shows the bound for $\#\mathcal{H}_0^{-1}(x_0)$.

# Thank You!

Questions?