ECFFT: An example

Harshit Bajpai

September 2022

1 Summary

1. Field $= F_p$, where $p = 997$
2. Maximum number of evaluation point $= 2^{10}$
3. Base elliptic curve $E_0 : Y^2 = X^3 + X^2 + 16X$
4. Order of base elliptic curve $= |E_0(F_{997})| = 2^{10}$

2 Good Curve and Good Point

Our field is an odd characteristic field so, Let

$$E_{a,B} : Y^2 = X^3 + aX^2 + BX$$

for non singularity $B, a^2 - 4B \neq 0$. The curve $E_{a,B}$ is said to be good if $B = b^2 \neq 0$ is a non zero quadratic residue and $a + 2b$ is a quadratic residue. In this case $P = (b, b\sqrt{a + 2b})$ is a good point of the curve.
As we know 9 and 16 are two non zero quadratic residues over modulo 997, So let

$$B = 16 \qquad a + 2b = 9$$

So,

$$b = 4 \qquad a = 1.$$

Hence our E_0 is,

$$E_0 : Y^2 = X^3 + X^2 + 16X$$

and the good point $P = (b, b\sqrt{a + 2b}) = (4, 12)$.

3 Good Isogeny

Let $E = E_{a,b^2}$ be a good curve in odd characteristic, with a good point P. Let $E^{'} = E_{a+6b,4ab+8b^2}$. Then there is a 2-isogeny $\phi = \phi_b : E \to E^{'}$ given by

$$\phi(x, y) = (x - 2b + \frac{b^2}{x}, (1 - \frac{b^2}{x^2})y).$$

Furthermore, we have $ker\phi = \{0, \infty\}$ and $\phi^{-1}(0) = \{P, -P\}$.
So transform

$$a \to a + 6b \qquad and \qquad b^2 \to 4ab + 8b^2$$

repeatedly until the size of cyclic subgroup remains 2, we get a ladder of good elliptic curves.

4 Construction of cyclic groups and isogeny chain

Suppose E_0 is a base elliptic curve as defined above. Now to construct cyclic groups and isogeny chain do the following:

1. Find an element g_0 of maximum order of the type 2^k in elliptic curve group.

2. Generate a cyclic subgroup G_0 of elliptic curve group E_0 using g_0.
   i.e, $G_0 =< g_0 >$ so $|G_0| = 2^k$.

3. Now calculate $P_0 = 2^{k-2}g_0$ and check whether P_0 is same as P defined above.

4. If $P_0 \neq P$ then transform base curve with $X^{'}$ and $Y^{'}$ defined as

   $$X^{'} = X - x_0 \qquad\qquad Y^{'} = Y$$

   Where x_0 is the x-coordinate of $2P_0 = (x_0, 0)$ (y-coordinate of $2P_0$ is zero because $2P_0$ is the 2- torsion point for the given representation). Thus in these coordinates the equation of the curve takes the form:

   $$Y^{'^2} = X^{'^3} + a_2'X^{'^2} + a_4'X'$$

   and $2P_0' = 0$, i.e. P_0' is a good point. Then do the same as defined in 5th point.

5. If $P_0 = P$ then by the 2-isogeny $\phi : E_0 \to E'$ as defined above, we have $\phi(0) = \infty, \phi(P_0) = 0$. It follows that $g_1 = \phi(g_0)$ generates a cyclic group of order 2^{k-1} inside E' and satisfies $P_1 = 2^{k-1-2}g_1$ (good point of E' with $2P_1 = 0$).

6. General iteration,
   for $0 \leq i \leq k-2$, we have a curve E_i with a point g_i of order $2^{k-i}$and a good point $P_i = 2^{k-i-2}g_i$ satisfying $2P_i = 0$.

7. Isogeny chain,
   for $0 \leq i \leq k-2$, we have a good 2-isogeny $\phi_i : E_i \to E_{i+1}$ with $g_{i+1} = \phi_i(g_i)$ such that $|g_{i+1}| = 2^{k-i-1}$ satisfying $2^{k-i-2}g_{i+1} = 0$.

8. Final curve E_{k-1} need not necessarily be good, and b_{k-1} is not necessarily defined, but b_{k-1}^2 is stil meaningful.

5 Projection and rational maps

Considering the x-projection map $\pi_i : E_i \to P^1 = F_{997} \cup \infty$, the x-coordinate of ϕ_i is a degree 2 rational map $\psi_i : P^1 \to P^1$ given by

$$\psi_i(x) := \begin{cases} \frac{(x-b_i)^2}{x} & \text{x} \notin \{0, \infty\} \\ \infty & \text{x} \in \{0.\infty\} \end{cases}$$

6 An isogeny chain

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_0"] \arrow[d, "\pi_0"'] & E_1 \arrow[r, "\varphi_1"] \arrow[d, "\pi_1"'] & \cdots \arrow[r, "\varphi_{k-2}"] & E_{k-1} \arrow[d, "\pi_k"] \\ \mathbb{P}^1 \arrow[r, "\psi_0"] & \mathbb{P}^1 \arrow[r, "\psi_1"] & \cdots \arrow[r, "\psi^{(k-2)}"] & \mathbb{P}^1 \end{tikzcd}$$

For our example we have $k = 9$ and the chain of elliptic curve is given as:

$$E_{1,16} \to E_{25,144} \to E_{97,358} \to E_{299,307} \to .....$$

7 Special sets in E_i and F_{997}

Let $E_0, E_1, ..., E_{k-1}$ be a sequence of elliptic curve as defined above with cyclic subgroups $G_i =< g_i >$ of size 2^{k-i} and a good point $P_i = 2^{k-i-2} g_i$. Define for each $i \leq k-1$,

1. $G'_i = G_i - \{0, \infty\} = G_i - \{2^{k-i-1} g_i, 2^{k-i} g_i\} \implies |G'_i| = |G_i| - 2 = 2^{k-i} - 2$.
2. $H_i = \pi_i(G_i) \implies |H_i| = 2^{k-i-1} - 1$.
3. $M_i = F_{997}[X]^{2^{k-i-1}}$ for every $i \leq k-1$. (It is a 2^{k-i-1}-dimensional space of polynomial of degree strictly less than 2^{k-i-1}.)

8 Evaluation Domain

Let Q_0 be a point on E_0 such that $2Q_0 \notin 2G_0 =< 2g_0 >$. Then the basic set corresponding to Q_0 is -

$$S_0 = S_0(Q_0) = (Q_0 + < 2g_0 >) \cup (-Q_0 + < 2g_0 >)$$

Since $2Q_0 \notin 2G_0, S_0$ is the union of two distinct coset of $2G_0$.
$\implies |S_0| = 2^{k-1} + 2^{k-1} = 2^k$.

Define inductively for $0 \leq i \leq k-2$,

$$Q_{i+1} = \phi_i(Q_i)$$

$$S_{i+1} = Q_{i+1}(S_i) = (Q_{i+1} + < 2g_{i+1} >) \cup (-Q_{i+1} + < 2g_{i+1} >)$$
$$\implies |S_{i+1}| = 2^{k-i-2} + 2^{k-i-2} = 2^{k-i-1}.$$

Define

$$T_i = \pi_i(S_i) \qquad for \qquad 0 \leq i \leq k-1.$$

We also write

$$T_{i+1} = \psi_i(T_i).$$

"S_i are disjoint from G_i, and thus similarly T_i are disjoint from H_i".

Our evaluation domain will be made from union of disjoint basic sets. For a set of points

$$\hat{Q}_0 = \{Q_{0,1}, Q_{0,2}, ...Q_0, m\} \in E_0$$

such that corresponding basic sets are all pairwise disjoint,
Let

$$\hat{S}_0 = \bigcup_{i=1}^{m} S_{0,i} = \bigcup_{i=1}^{m} S_0(Q_{0,i})$$

$$\hat{T}_0 = \bigcup_{i=1}^{m} T_{0,i} = \bigcup_{i=1}^{m} \pi_0(S_{0,i})$$

again define $\hat{Q}_i, \hat{S}_i, \hat{T}_i$ recursively as above using ψ_i, π_i, ϕ_i we will have

$$|\hat{S}_i| = 2^{k-i}m \qquad |\hat{T}_i| = 2^{k-i-1}m.$$

9 ECFFT

Let $Q_i \in E_i$ generates an orbit S_i of size 2^{k-i} and let $T_i = \pi_i(S_i)$ and let B_i be the standard basis of M_i then there exist invertible linear transformations FFT and $IFFT$ such that $\forall f$

$$FFT([f]_{B_i}) = < f \wr T_i >, \qquad IFFT(< f \wr T_i >) = [f]_{B_i}$$

Where,

$$[f]_{B_i} = \sum c_j x^j$$

$$< f \wr T_i > = evaluation \ \ of \ \ f \ \ over \ \ T_i.$$

These $FFTs$ and their inverses are analogous to the usual FFT. The main difference is that for standard FFT, the basis for the space of polynomials is the standard basis, so [f] is simply the vector of coefficients of monomials, whereas in the EC case the "natural" basis is more complicated. The circuit itself is very similar, consisting of $N/2$ butterflies in each of the $log_2 N$ layers, each layer

using a different stride size. The only difference between these butterflies and those of the usual FFT is in the twiddle factors used: the values of ζ_i at the points of T_i, instead of roots of unity (or a coset). These values are determined by a precomputation, which the FFT/IFFT circuit need not be aware of.
Processes of evaluation,

$$f(x) = f_0(\psi_i(x)) + \zeta_i(x) f_1(\psi_i(x))$$

Let $x_0, x_1 \in T_i$ be any pair with $\psi_i(x_0) = \psi_i(x_1) = x'$. Such pairs satisfies $x_0 x_1 = b_i^2$, so $x' = x_0 + x_1 - 2b_i$ and they can be easily located as they are always at distance $\frac{|T_i|}{2}$ from each other when ordered according to the coset. Substituting $x = x_0, x_1$ we find

$$f(x_0) = f_0(x') + \zeta_i(x_0) f_1(x'), \qquad f(x_1) = f_0(x') + \zeta_i(x_1) f_1(x')$$

Since ζ_i is a degree-1 rational function, it is one-one, thus $\zeta_i(x_0) \neq \zeta_i(x_1)$ so the system of equation given above is invertible, allowing to solve $f_0(x'), f_1(x')$ from $f(x_0), f(x_1)$. When $\zeta_i(x_0), \zeta_i(x_1)$ are nicely related, the inversion formula can also be simplified. If $\zeta_i(x_1) = -\zeta_i(x_0)$ then

$$f_0(x') = \frac{f(x_0) + f(x_1)}{2} \qquad f_1(x') = \frac{f(x_0) - f(x_1)}{2\zeta_i(x_0)}$$

We can thus exchange between $f(x_0), f(x_1)$ and $f_0(x'), f_1(x')$ in O(1) operations. More specifically, assuming precomputation of values of the $\zeta_i(x_0)$ and their inverses, we use only 1 multiplication and 2 additions/subtractions for each pair.