# Contents



# 1 Frobenius

$$\Phi_{q^k} : \bar{\mathbb{F}}_{q^k} \to \bar{\mathbb{F}}_{q^k}$$

$$\Phi(x) = x^{q^k}$$

$$\text{Fixed}(\Phi_{q^k}) = \mathbb{F}_{q^k} \subseteq \bar{\mathbb{F}}_{q^k}$$

# 2 Find Pairing Friendly Groups

**Def**: Let $q$ be a prime. We say that an EC E/ _q is pairing friendly if

1. There exists a prime $r > \sqrt{q}$ such that $r|\#E(\mathbb{F}_q)$
    1. Estimation in hasse-weil theorem we see $\#E(\mathbb{F}_q) = q+1-t$ where $|t| \leq 2\sqrt{q}$ which is roughly $q \pm 2\sqrt{q}$.
2. The embedding degree of $E$ wrt $r$ satisfies $k \leq \log_2(r)/8$.

We want a *type II* pairing of order $r$.

$$e : G_1 \times G_2 \to G_T$$

$$r = |G_1| = |G_2| = |G_T|$$

**Last time**: For nice $r$ we can write

$$E[r] \cong H_1 \times H_q$$

$$= E(\mathbb{F}_q)[r] \times \text{Eig}_q(\Phi_q) \cap E[r]$$

Note: $|H_1| = |H_q| = r$ since $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$.

if $|H_1| = r^2$ then $E[r] \subseteq E(\mathbb{F}_q)$ so $k = 1$.

Natural choices

$$G_T = \mu_r$$

$$G_1 = E(\mathbb{F}_q)[r]$$

$$G_2 = \ker(\Phi - [q]) \cap E[r] \subseteq E(\mathbb{F}_{q^k})$$

# 3 How to find $G_1$?

Denote $\#E(\mathbb{F}_q) = hr$, where $h$ is the cofactor. Take any $P \in E(\mathbb{F}_q)$ and check if $hP \neq \infty$. If so $hP$ is a generator of $G_1$.

# 4 Efficient Representation of $G_2$

**Thm:** Let $E/\mathbb{F}_q$ where $q = p^n$ is a prime power, so the trace of Frobenius $t \neq 0 \bmod p$. Let $d \in \{2, 3, 4, 6\}$ (possible degrees of twists) and $r > d$ a prime with $r | \#E(\mathbb{F}_q)$ and $r^2 | E(\mathbb{F}_{q^d})$ with $d$ minimal.

Then there is a unique degree $d$ twist $E'$ of $E$ such that $r | E'(\mathbb{F}_q)$, and the twist

$$\varphi_d : E'(\mathbb{F}_q) \to E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k})$$

is a monomorphism that maps an order $r$ subgroup $G_2'$ of $E'(\mathbb{F}_q)$ isomorphically to $G_2$.

$$G_2 = \ker(\Phi - [q]) \cap E[r] \subseteq E[r] \subseteq E(\mathbb{F}_{q^k})$$

# 5 Construction

Assume $E$ admits a degree $d$ twist. Let $m = \gcd(k, d)$ and $e = k/m$. Then there is a unique degree $m$ twist $E'$ of $E$ over $\mathbb{F}_{q^e}$ such that $r | \#E'(\mathbb{F}_{q^e})$ and denoted by

$$\varphi_m : E'(\mathbb{F}_{q^e}) \to E(\mathbb{F}_{q^{em}}) = E(\mathbb{F}_{q^k})$$

which is a monomorphism that maps $G_2' \subseteq E'(\mathbb{F}_{q^e})$ isomorphically to $G_2 \subseteq E(\mathbb{F}_{p^k})$.

Then we obtain a modified type II pairing

$$\bar{e} : G_1 \times G_2' \to G_T$$

$$\bar{e}(P, Q') = e(P, \varphi_m(Q'))$$

where $\varphi_m(Q') = Q$.

e.g BLS12-381, $k = 12, E : y^2 = x^3 + 4$ where $j(E) = 0$. So there exists $d = 6$ twist of $E \Rightarrow m = \gcd(k, d) = 6$, $e = k/m = 2$ so there exists $d = 6$ twist $E'$ of $E$ over $\mathbb{F}_{q^e} = \mathbb{F}_{q^2}$ with $G_2' \subseteq E'(\mathbb{F}_{q^2})$.

there exists an explicit formula for the twist

$$\varphi_m : E'(\mathbb{F}_{q^2}) \to E(\mathbb{F}_{q^k})$$

# 6 BLS12-381

This is a parameterized family of pairing-friendly curves.

$$r(X) = X^4 - X^2 + 1$$
$$t(X) = X + 1$$
$$q(X) = \frac{(X-1)^2}{3}(X^4 - X^2 + 1) + X$$

with $E : y^2 = x^3 + 4$ with the parameter $X$. Embedding degree is always $k = 12$.

There is a known value $X$ that gives the largest $r(X)$. Which gives us $q = 381$ bits.

Note: $j(E) = 0 \left(= \frac{4A^3}{4A^3+27B^2} 1728\right)$ but $A = 0$.

So there is a sextic twist of $E$.

Thus $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$ and

$$\mathbb{G}_2 = \ker(\Phi - [q]) \cap E[r]$$

and $\mathbb{G}_2$ can be represented by $\mathbb{G}_2' \subseteq E(\mathbb{F}_{q^2})$ via an isomorphism

$$\varphi_m : \mathbb{G}_2' \to \mathbb{G}_2$$

$$E(\mathbb{F}_{q^2}) \to E(\mathbb{F}_{q^{12}})$$

Thus there exists a degree 6 twist $\varphi_6$ of $E$ over $\mathbb{F}_{q^2}$.

And hence a more efficient modified pairing:

$$\bar{e} : \mathbb{G}_1 \times \mathbb{G}_2' \to \mathbb{G}_T = \mu_r$$

$$\bar{e}(P, Q') = e(P, \varphi_6 Q')$$

# 7 How to represent $\mathbb{F}_{q^2}$?

**Lemma:** let $q$ be a prime, then the polynomial $g(x) = x^2 + 1$ is irreducible iff $q \neq 1 \mod 4$.

Otherwise let $\alpha$ be a root of $g$. Then $\alpha^2 = -1$, so $\alpha^4 = 1$ and so $4 || \mathbb{F}_q^\times | \Leftrightarrow 4 | (q-1) \Leftrightarrow q \equiv 1 \mod 4$.

In BLS for the ideal $X$, $q \equiv \mod 4$.

$$\mathbb{F}_{q^2} = \mathbb{F}_q[x]/\langle x^2 + 1 \rangle$$

with this representation

$$E' : y^2 = x^3 + 4(i+1)$$