Moonmath manual

TechnoBob and the Least Scruples crew

July 31, 2021

Lorem **ipsum** dolor sit amet, consectetur adipiscing elit. Pellentesque semper viverra dictum. Fusce interdum venenatis leo varius vehicula. Etiam ac massa dolor. Quisque vel massa faucibus, facilisis nulla nec, egestas lectus. Sed orci dui, egestas non felis vel, fringilla pretium odio. *Aliquam* vel consectetur felis. Suspendisse justo massa, maximus eget nisi a, maximus gravida mi.

Here is a citation for demonstration: **?**

Pairings

In this chapter, we discuss *pairings*, which form the basis of several zk-SNARKs and other zero knowledge proof schemes. The SNARKs derived from pairings have the advantage of constant-sized proof sizes, which is crucial to blockchains.

We start out by defining pairings and discussing a simple application which bears some resemblance to the more advanced SNARKs. We then introduce the pairings arising from elliptic curves and describe Miller's algorithm which makes these pairings practical rather than just theoretically interesting.

0.0.1 Bilinear Pairings

Definition 0.0.1. For finite abelian groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, a *pairing*

$$\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

is a map with the following properties.
1. Bilinearity: $\mathbf{e}(x_1+x_2, y_1+y_2) = \mathbf{e}(x_1,y_2)\cdot\mathbf{e}(x_1,y_2)\cdot\mathbf{e}(x_2,y_1)\cdot\mathbf{e}(x_2,y_2)$
$\forall\, x_1,x_2 \in \mathbb{G}_1,\ y_1,y_2 \in \mathbb{G}_2$.
2. Non-degeneracy: The image of $\mathbf{e}$ is non-trivial.
3. Efficient computability.

In pairing-based cryptography, we typically work in settings where the groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic of order p for some 256-bit prime p so as to have a 128-bit security level. Such pairings $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ are classified into three types:
- Type I: $\mathbb{G}_1 = \mathbb{G}_2$.
- Type II: $\mathbb{G}_1 \neq \mathbb{G}_2$ but there is an *efficiently computable* isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$.
- Type III: There is no *efficiently computable* isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$.

In particular, for elements $x_1, y_1 \in \mathbb{G}_1$, $x_2, y_2 \in \mathbb{G}_2$, we have $e(x_1,y_1) = \mathbf{e}(x_2,y_1) \in \mathbb{G}_T$ if and only if there exists an integer $s \in [0, p-1]$ such that $y_1 = x_1^s$ and $y_2 = x_2^s$. This simple fact is deceptively powerful and lies at the heart of several zero-knowledge proof schemes. In all of the existing pairing based SNARKs and zero knowledge proof systems, the pairings are performed by the *Verifier* rather than the Prover. Thus, it is fundamentally important for the pairings to be efficient.

At present, the only efficient pairings that we know of are those arising from (Jacobians of) hyperelliptic curves over finite fields. The most efficient of these are the ones arising from elliptic curves, i.e. hyperelliptic curves of genus one. The fact that elliptic curves - which were pivotal to cryptography even before pairings gained traction - are the best known source of pairings seems to be a happy coincidence.

Cryptographic assumptions

We state the computationally infeasible problems that the security of pairing-based SNARKs hinges on.

Assumption 0.0.1. ***n*-strong Diffie Hellman assumption:** *Let $\mathbb{G}$ be a cyclic group of prime order p generated by an element g, and let $s \in \mathbb{F}_p^*$. Any probabilistic polynomial-time algorithm that is given the set $\{g^{s^i} : 1 \leq i \leq n\}$ can find a pair $(a, g^{1/(s+a)}) \in \mathbb{F}_p^* \times \mathbb{G}$ with at most negligible probability.*

Assumption 0.0.2. Knowledge of exponent (KEA) assumption:. *Let $\mathbb{G}$ be a cyclic group of prime order p generated by an element g, and let $s \in \mathbb{F}_p^*$. Suppose there exists a PPT algorithm $\mathscr{A}_1$ that given the set $\{g^{s^i}, g^{s^i\alpha} : 1 \leq i \leq n\}$, outputs a pair $(c_1,c_2) \in \mathbb{G}\times\mathbb{G}$ such that $c_2 = c_1^\alpha$. Then there exists a PPT algorithm $\mathscr{A}_2$ that, with overwhelming probability, outputs a polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $\leq n$ such that $c_1 = g^{f(s)}$, $c_2 = g^{\alpha f(s)}$.*

The n-strong Diffie Hellman is a stronger assumption than the older and more battle-tested discrete logarithm assumption in elliptic curves. The KEA assumption is even younger and is unfalsifiable. This is one of the downsides to pairing-based SNARKs when compared to schemes such as Bulletproofs, DARK etc. that do not rely on pairings.

Membership proofs

As a warmup, we discuss a simple example of an application of pairings, namely set membership proofs. This could be though of as an application specific SNARK and is substantially simpler than the Groth16 Snark which we will discuss in subsequent chapters. But it shares a common structure with the more advanced SNARKs in that
- the Prover's work is dominated by elliptic curve operations and Fast Fourier transforms
- the Verifier's work is dominated by elliptic curve pairings
- the scheme requires a trusted setup for the common reference string (CRS), which in practice is generated via a multi-party computation
- the security hinges on the KEA and strong Diffie-Hellman assumptions

We describe the setup in this section. Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be cyclic groups of order p for some prime p such that there exists a pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ which is *bilinear*, *non-degenerate* and *efficiently computable*. Fix generators g_1, g_2 of the cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ respectively. Then $\mathbf{e}(g_1, g_2)$ is a generator of $\mathbb{G}_T$. Unlike in the case of accumulators based on groups of unknown order, the (common) order of the groups is public. Instead, the secret trapdoor is an integer s in the range $[1, p-1]$ which will serve as the private key. Unfortunately, the generation of the private key requires a trusted setup. This can be partially mitigated by using a secure multi-party computation. A Verifier needs to assume that at least one of the parties involved in the MPC is honest enough not to collude with the other participants.

For a data set $\mathscr{D} = \{d_1, \cdots, d_n\}$, we define the accumulated digest

$$\mathrm{Acc}(\mathscr{D}) := g_1^{\prod\limits_{d \in \mathscr{D}} (d+s)} \in \mathbb{G}_1.$$

For a subset $\mathscr{D}_0 \subseteq \mathscr{D}$, the witness for $\mathscr{D}_0$ is defined by

$$\mathrm{Wit}(\mathscr{D}_0) := g_1^{\prod\limits_{d \in \mathscr{D} \setminus \mathscr{D}_0} (d+s)}.$$

The Verifier then needs to check whether

$$\mathrm{Wit}(\mathscr{D}_0)^{\prod\limits_{d_0 \in \mathscr{D}_0} (d_0+s)} = \mathrm{Acc}(\mathscr{D}).$$

Because of the bilinearity of the pairing, it is equivalent and usually more efficient to verify the following equation:

$$\mathbf{e}\Big(\mathrm{Wit}(\mathscr{D}_0)\ ,\ g_2^{\prod\limits_{d_0 \in \mathscr{D}_0} (d_0+s)}\Big) = \mathbf{e}(\mathrm{Acc}(\mathscr{D}), g_2).$$

Since none of the parties are aware of the value of s, it is necessary to broadcast the sets $\{g_1, g_1^s, \cdots, g_1^{s^n}\}$ and $\{g_2, g_2^s, \cdots, g_2^{s^n}\}$ to the Prover.

In the orignal bilinear accumulator scheme, the Verifier needs access to the sets $\{g_1, g_1^s, \cdots, g_1^{s^n}\}$ and $\{g_2, g_2^s, \cdots, g_2^{s^n}\}$. But we can modify the scheme so that the Verifier only needs the four points $\{g_1, g_1^s, g_2, g_2^s\}$ to verify membership or non-membership.

The exponent $\prod\limits_{d \in \mathscr{D}} (d+s)$ can be interpreted as a degree n polynomial in the variable s. The coefficients of the polynomial are computed with a run time of $\mathbf{O}(n\log(n))$ using the Fast Fourier transform. Furthermore, the set $\mathbb{F}_p[X]$ of polynomials with $\mathbb{F}_p$-coefficients is a principal ideal domain whose maximal ideals are those generated by the irreducible polynomials. For a data set $\mathscr{D}$, the polynomial $f(X) = \prod\limits_{d \in \mathscr{D}} (X+d)$ is monic of degree $n = |\mathscr{D}|$. Let c_i denote the coefficient of X^i, i.e. $f(X) = \sum\limits_{i=0}^{n} c_i X^i$. The coefficients can be computed in run time $\mathbf{O}(n\log(n))$ using the Fast Fourier transform. The elements

$$g_1^{f(s)} = \prod_{i=0}^{n} (g_1^{s^i})^{c_i} \ \in \mathbb{G}_1 \ \ , \ \ g_2^{f(s)} = \prod_{i=0}^{n} (g_2^{s^i})^{c_i} \ \in \mathbb{G}_2$$

can then be computed by any party that possesses the elements $\{g_1^{s^i}, g_2^{s^i} : \ 0 \leq i \leq n\}$. The collision-resistance of the bilinear accumulator hinges on the n-Strong Diffie Hellman assumption.

Protocol 0.0.1. *Proof of exponent for pairings* (PoE)*:*
Parameters : A pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ of groups of prime order p; generators g_1, g_2 of $\mathbb{G}_1$, $\mathbb{G}_2$ respectively; a secret element $s \in \mathbb{F}_p^*$ such that the Prover possesses the elements $\{g_1^{s^i}, g_2^{s^i} : 0 \leq i \leq n\}$
Inputs: $a, b \in \mathbb{G}_1$; a polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $\leq n$
Claim: $a^{f(s)} = b$

1. The Fiat-Shamir heuristic generates a challenge $\alpha \in \mathbb{F}_p^*$ (the challenge).
2. The Prover computes a polynomial $h(X) \in \mathbb{F}_p[X]$ and an element $\beta \in \mathbb{F}_p^*$ such that $f(X) = (X+\alpha)h(X) + \beta$. The Prover sends $Q := a^{h(s)}$ to the Verifier.
3. The Verifier computes $\beta := f(X) \pmod{(X+\alpha)}$ and accepts if and only if the equation

$$\mathbf{e}(Q, g_2^{s+\alpha}) \cdot \mathbf{e}(a, g_2^{\beta}) = \mathbf{e}(b, g_2)$$

holds. □

We use the last protocol to modify the proof of membership for a data set.

Protocol 0.0.2. *Protocol for set membership.*
Parameters : A pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ of groups of prime order p; generators g_1, g_2 of $\mathbb{G}_1$, $\mathbb{G}_2$ respectively; a trapdoor $s \in \mathbb{F}_p^*$ such that the Prover possesses the elements $\{g_1^{s^i}, g_2^{s^i} : 0 \leq i \leq n\}$ and the Verifier possesses the set $\{g_1, g_2, g_1^s, g_2^s\}$
Inputs: Data sets $\mathscr{D}$, $\mathscr{D}_0$; the accumulated digest $\mathrm{Acc}(D)$
Claim: $\mathscr{D}_0 \subseteq \mathscr{D}$.

1. The Prover computes the polynomial $f_0(X) := \prod_{d_0 \in \mathscr{D}_0} (X + d_0)$.
2. The Prover computes

$$\mathrm{Wit}(\mathscr{D}_0) := g_1^{\prod_{d \in \mathscr{D} \setminus \mathscr{D}_0} (d+s)}.$$

3. The Prover sends the Verifier a non-interactive PoE for the equation $\mathrm{Wit}(\mathscr{D}_0)^{f_0(s)} = \mathrm{Acc}(\mathscr{D})$.
4. The Verifier computes $f_0(X)$ and accepts if and only if the PoE is valid. □

0.0.2 Pairings from elliptic curves

The Weil number: An elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p is endowed with the endomorphism

$$\mathrm{Fr}_E : E \longrightarrow E \ , \ (x, y) \longrightarrow (x^p, y^p).$$

This endomorphism is called the *Frobenius* endomorphism of E and satisfies a quadratic equation $X^2 - tX + q$ for some integer t. This endomorphism commutes with every endomorphism of E. Furthermore, the Frobenius of any elliptic curve isogenous to E satisfies the same quadratic equation.

A Weil q-integer is an algebraic integer α such that $\sigma(\alpha) \cdot \overline{\sigma(\alpha)} = q$ for every automorphism $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Thus, the Frobenius of an elliptic curve is a Weil q-integer π such that $[\mathbb{Q}(\pi) : \mathbb{Q}] \leq 2$. From Honda-Tate theory, we know that the map $E \longrightarrow \mathrm{Fr}_E$ yields a bijection

$$\{\text{Elliptic curves } \mathbb{F}_q \text{ up to isogeny}\} \longrightarrow \left\{ \begin{array}{l} \text{Weil } q\text{-integers } \pi \text{ such that } [\mathbb{Q}(\pi) : \mathbb{Q}] \leq 2 \\ \text{up to conjugacy} \end{array} \right\}$$

Torsion subgroups: For any integer n prime to p, the n-torsion subgroup $E(\overline{\mathbb{F}}_p)[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. For any prime power p^k, the p^k-torsion is either trivial or cyclic of order p^k. In the former case, E is said to be *supersingular* while in the latter case it is said to be *ordinary*.

As the etymology suggests, most elliptic curves are ordinary. In fact, up to isogeny, there is a unique supersingular elliptic curve over the algebraic closure $\overline{\mathbb{F}}_p$. In fact, E is supersingular if and only if:
- its Weil number π is an algebraic integer of degree ≤ 2
- $\pi^k \in \mathbb{Z}$ for some integer $k \geq 1$.

Clearly, such Weil numbers - and consequently supersingular curves - are rare. Since Type I and II pairings require supersingular elliptic curves, this is yet another reason to use type III pairings instead.

Endomorphisms: For an elliptic curve E, an endomorphism ϕ of E is an algebraic map $\phi : E \longrightarrow E$. The set of endomorphisms of E is called the endomorphism ring of E (denoted by (E)). It has the structure of a ring with no zero-divisors that is finite dimensional over $\mathbb{Z}$-module. The tensor product ${}^0(E) := (E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is called the endomorphism algebra. The center of (E) is the subring $\mathbb{Z}[\pi_{_E}]$. Similarly, the field $\mathbb{Q}(\pi_{_E})$ is the center of the division algebra ${}^0(E)$. For simplicity, we assume the field $\mathbb{F}_q$ has been enlarged to endure that $(E) = (E \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q)$. Broadly, ${}^0(E)$ has one of two possible structures:
1. If E is ordinary, ${}^0(E) = \mathbb{Q}(\pi_{_E})$ and is an imaginary quadratic field in which the prime p splits. Thus, (E) is an order (not necessarily maximal) in this imaginary quadratic field.
2. If E is supersingular, $\pi_{_E} = \sqrt{q} \in \mathbb{Z}$ and ${}^0(E)$ is the quaternion algebra $\mathbb{Q}_{p,\infty}$ ramified exclusively at p and $\infty_{_E}$. The endomorphism ring (E) is a maximal order in $\mathbb{Q}_{p,\infty}$.

Examples: 1. Consider an elliptic curve

$$E : y^2 = x^3 + ax$$

over a prime field $\mathbb{F}_p$ for some $a \in \mathbb{F}_p^*$. In addition to the endomorphisms

$$E \longrightarrow E \ \ , P \mapsto [n]P \quad (n \in \mathbb{Z}),$$

the curve is endowed with the endomorphism

$$(x_1, y_1) \mapsto (x_1, y_1 \cdot \sqrt{-1}).$$

Thus, E has action by $\mathbb{Z}[\sqrt{-1}]$.

2. Consider an elliptic curve

$$E : y^2 = x^3 + a$$

over a prime field $\mathbb{F}_p$ for some $a \in \mathbb{F}_p^*$. In addition to the scalar multiplication endomorphisms, the curve is endowed with the endomorphism

$$(x_1, y_1) \mapsto (x_1, y_1 \cdot \zeta_3).$$

Thus, E has action by $\mathbb{Z}[\zeta_3]$.

We note that we are abusing notation by using $\sqrt{-1}$ for a square root of -1 in $\overline{\mathbb{Q}}$ as well as $\overline{\mathbb{F}}_p$. Likewise, we have denoted a cube root of unity in $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_p$ by ζ_3.

The embedding degree: Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Let π be the Weil number associated to E. Then π is an algebraic integer such that $\pi \cdot \overline{\pi} = q$ and $\pi + \overline{\pi} \in \mathbb{Z}$. Furthermore, the number of $\mathbb{F}_{q^k}$-points on E is given by $|(1-\pi^k)(1-\overline{\pi}^k)|$.

Now, suppose $\ell \neq p$ is a prime dividing $\#E(\mathbb{F}_q)$. This is equivalent to there existing a prime $\mathfrak{l}$ of $\mathbb{Q}(\pi)$ lying over ℓ such that $\pi - 1 \in \mathfrak{l}$. For simplicity, assume ℓ^2 does not divide $\#E(\mathbb{F}_q)$, which means:
- ℓ splits into two distinct prime ideals $\mathfrak{l}, \bar{\mathfrak{l}}$ in $\mathbb{Q}(\pi)$.
- $\pi - 1 \notin \mathfrak{l}^2 \cup \bar{\mathfrak{l}}$.

The ℓ-torsion group $E(\overline{\mathbb{F}}_p)[\ell]$ is given by

$$E(\overline{\mathbb{F}}_p)[\ell] = E(\overline{\mathbb{F}}_p)[\mathfrak{l}] \oplus E(\overline{\mathbb{F}}_p)[\bar{\mathfrak{l}}] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

The *embedding degree* of E with respect to ℓ is the integer k that satisfies one of the following equivalent conditions:

1. k is the smallest integer such that $q^k \equiv 1 \pmod{\ell}$.
2. k is the smallest integer such that $\overline{\pi}^k \equiv 1 \pmod{\mathfrak{l}}$
3. k is the smallest integer such that all ℓ-torsion points of E are defined over the extension $\mathbb{F}_{q^k}$.

4. $\Phi_k(q) \equiv 0 \pmod{\ell}$ where $\Phi_k(X)$ is the k-th cyclotomic polynomial.

We denote by $\mu_\ell(\mathbb{F}_{q^k})$ the unique cyclic subgroup of $\mathbb{F}_{q^k}^*$ of order ℓ. For a randomly chosen elliptic curve E, the embedding degree with respect to any prime dividing $\#E(\mathbb{F}_q)$ is quite large. In fact, the embedding degree is of the same order of magnitude as q. Elliptic curves that are amenable to pairings (aka pairing-friendly curves) are rare.

We now briefly describe the pairings associated with an elliptic curve over a finite field. To this end, we first describe divisors on curves.

0.0.3 Divisors

We start out by defining divisors on elliptic curves. Most of the concepts here generalize to arbitrary smooth curves over perfect fields. But we will confine our focus to divisors on elliptic curves over finite fields.

Let E be an elliptic curve over a finite F with Weierstrass equation $r(X,Y) = 0$. Let $\overline{F}$ denote the algebraic closure of F. We denote by $E(\overline{F})$ the group of $\overline{F}$-points of E.

A *divisor* D on E is a formal sum $\sum_{P \in E} n_{D,P}(P)$ where the n_P are integers that are non-zero for at most finitely many points P. The set of points P such that $n_{D,P} \neq 0$ is called the *support* of D and is denoted by $\mathrm{supp}(D)$. The sum $\sum_{P \in E} n_{D,P}$ is called the *degree* of D.

The divisor $\varepsilon(D) := \sum_{P \in E, n_{D,P} \geq 0} n_{D,P} P$ is called the *effective* part of D. The divisor D is said to be *effective* if $\varepsilon(D) = D$. Clearly, any divisor can be realized as the difference between two effective divisors.

Thus, the set of divisors on E has the structure of an abelian group and is naturally endowed with an action by Gal_F. We say a divisor D is defined over K if $D = \sigma(D)$ for every $\sigma \in \mathrm{Gal}_F$. The set of divisors defined over F is denoted by $\mathrm{Div}_F(E)$. This is a subgroup of $\mathrm{Div}(E)$.

The degree zero divisors defined over F form a subgroup of $\mathrm{Div}_F(E)$. We denote this subgroup by $\mathrm{Div}_F^0(E)$. The *function field* of E over F is the field of fractions $F(E)$ of the integral domain $F[X,Y]/r(X,Y)$. The divisor of a function $f \in F(E)$ is given by $\mathrm{div}(f) := \sum_P m_{f,P}(P)$ where $m_{f,P}$ is the multiplicity of P as a zero of f.

A divisor is said to be *principal* if it occurs as the divisor of some rational function. The set of divisors of functions has the structure of a group. Furthermore, a divisor $D = \sum_{P \in E} m_{D,P}(P)$ is principal if and only if $\sum_{P \in E} m_{D,P} = 0$ and $\sum_{P \in E} n_{D,P}(P) = \infty_E$. Thus, every principal divisor has degree zero. We denote the set of principal divisors by $\mathrm{Prin}(E)$. This is a subgroup of $\mathrm{Div}^0(E)$.

The quotient $\mathrm{Div}^0(E)/\mathrm{Prin}(E)$ is called the *divisor class group* or the Picard group of E and is denoted by $\mathrm{Pic}^0(E)$. For elliptic curves, $\mathrm{Pic}^0(E)$ has a canonical isomorphism with E. For higher genus curves, $\mathrm{Pic}^0(C)$ is not in bijection with C but has the structure of an *abelian variety*, a protective variety with a group structure.

For a function $f \in \mathbb{F}_q(E)$ and a divisor $D = \sum_P m_{f,P} P$ such that D, (f) have disjoint supports, we have

$$f(D) = \prod_P f(P)^{m_{f,P}}.$$

The *Weil reciprocity law* states that for non-zero functions f, g on the curve with disjoint supports,

$$f((g)) = g((f)).$$

We omit the details since that would be too great a digression but we note that this lies at the heart of many of the proofs of the pairing properties of elliptic curves.

For distinct points P, Q on the curve, we denote the line passing through them by $\mathscr{L}_{P,Q}$ (or $\mathscr{L}_{Q,P}$). We denote the tangent line to the curve at the point P by $\mathscr{L}_{P,P}$. We denote the vertical line passing through P

(and $-P$) by $\mathscr{V}_P$ (or $\mathscr{V}_{-P}$).

Pairings: Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Let π be the Weil number associated to E. Then π is an algebraic integer such that $\pi \cdot \overline{\pi} = q$ and $\pi + \overline{\pi} \in \mathbb{Z}$. Furthermore, the number of $\mathbb{F}_{q^k}$-points on E is given by $|(1-\pi^k)(1-\overline{\pi}^k)|$.

Now, suppose $\ell \neq p$ is a prime such that $\#E(\mathbb{F}_q) \in \ell\mathbb{Z} \setminus \ell^2\mathbb{Z}$. Then the ℓ-torsion group $E(\overline{\mathbb{F}}_p)[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ while $E(\mathbb{F}_q)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$. Let k be the embedding degree of E with respect to ℓ. We denote by $\mu_\ell(\mathbb{F}_{q^k})$ the unique cyclic subgroup of $\mathbb{F}_{q^k}^*$ of order ℓ.

The Tate pairing: Let $P \in E(\mathbb{F}_q)[\ell]$. Then there exists a rational function $f_{\ell,P}$ with divisor $(f_{\ell,P}) = \ell(P) - \ell(\infty_E)$. Let $Q \in E(\mathbb{F}_q)$ be any representative in the equivalence class $E(\mathbb{F}_{q^k})/\ell \cdot E(\mathbb{F}_{q^k})$. Let D_Q be a degree zero divisor defined over $\mathbb{F}_{q^k}$ that is equivalent to $(Q) - (\infty_E)$ but whose support is disjoint from that of $(f_{\ell,P})$. The (intermediate) Tate pairing t_ℓ is a map

$$t_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell \cdot E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell \ , \ (P,Q) \mapsto f_{\ell,P}(D_Q).$$

This pairing is bilinear and non-degenerate and the target group is the quotient group $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell$ which is cyclic of order ℓ.

A shortcoming of this pairing is that it is not entirely deterministic. Different parties may compute values that coincide under this notion of equivalence but are distinct in a stricter sense. To this end, we modify the definition by defining

$$T_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell \cdot E(\mathbb{F}_{q^k}) \longrightarrow \mu_\ell(\mathbb{F}_{q^k})$$

$$(P,Q) \mapsto t_\ell(P,Q)^{(q^k-1)/\ell} = f_{\ell,P}(D_Q)^{(q^k-1)/\ell}.$$

The last part is a (rather expensive) exponentiation in the finite field $\mathbb{F}_{q^k}$ and is called the *final exponentiation* for Tate pairings. It is one of the two components of a Tate pairing, the other being the Miller loops which we describe below.

The Weil pairing: Let $P, Q \in E(\mathbb{F}_{q^k})[\ell]$ and let D_P, D_Q be divisors with disjoint supports such that $D_P \sim (P) - (\infty_E)$, $D_Q \sim (Q) - (\infty_E)$. There exist rational functions $f_{\ell,P}$, $g_{\ell,P}$ such that $(f_{\ell,P}) = \ell \cdot D_P$, $(g_{\ell,P}) = \ell \cdot D_Q$. The Weil pairing is a map

$$w_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \longrightarrow \mu_\ell(\mathbb{F}_{q^k})$$

defined by

$$w_\ell(P,Q) := \frac{f_{\ell,P}(D_Q)}{g_{\ell,Q}(D_P)}.$$

This map is well-defined, i.e. the value $w_\ell(P,Q)$ is independent of the choice of the rational functions $f_{\ell,P}$, $g_{\ell,P}$. The Weil pairing is bilinear, non-degenerate and *alternating* in the sense that $w_\ell(P,P) = 1$ for any point P. Furthermore, $w_\ell(P,Q) = 1$ if and only if P and Q lie in the same cyclic group of order ℓ. Thus, choosing r-torsion points P, Q that generate distinct cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$ of order ℓ and setting $\mathbb{G}_T := \mu_\ell(\mathbb{F}_{q^k})$ yields a non-degenerate bilinear pairing

$$\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T.$$

Although the Tate and Weil pairings are significantly different, their computations have a common structure. The Weil pairing boils down to computing $f_{\ell,P}(D_Q)$, $g_{\ell,P}(D_P) \in \mathbb{F}_{q^k}^*$. The Tate pairing entails computing $f_{\ell,P}(D_Q) \in \mathbb{F}_{q^k}^*$ followed by the final exponentiation.

The security parameter: The integer $\frac{\ell-1}{k}$ is called the security parameter of E with respect to ℓ. The strongest attacks against the discrete logarithm problem in the ℓ-torsion subgroup of E are
- the MOV (Menezes Okamoto Vanstone) attack which has runtime complexity $\mathbf{O}(\frac{\ell-1}{k})$.
- the Kim-Barbelescu number field sieve attack that exploits the discrete log in the target group $\mathbb{G}_T$.

Thus, the integer $\frac{\ell-1}{k}$ has to be large enough for the scheme to be secure. Furthermore, k has to be sufficiently large so that the index calculus attack against the DLP in $\mathbb{F}_{q^k}^*$ is infeasible. On the other hand, the integer q^k has to be small enough for the arithmetic in the field $\mathbb{F}_{q^k}$ to be reasonably efficient. It appears that the golden mean lies at ordinary elliptic curves with embedding degree 12. For 128-bit security, we need the elliptic curve to be defined over a 380-bit prime and for the prime ℓ to be a 256-bit prime.

The curve E is said to be *pairing-friendly* if $\#E(\mathbb{F}_q)$ has a prime divisor ℓ such that:
- $\ell \geq \sqrt{q}$
- the embedding degree of E with respect to ℓ is $\leq \log_2(\ell)/8$

In practice, the curve most widely used for SNARKs is the BLS12-381, thus named because it is defined over a 381-bit prime field $\mathbb{F}_p$ and $\#E(\mathbb{F}_p)$ has a 256-bit prime divisor ℓ such that E has embedding degree 12 with respect to ℓ.

The BLS12-381 curve is given by the equation

$$E : y^2 = x^3 + 4$$

over a certain prime field $\mathbb{F}_p$ of bit-size 381. The group $E(\mathbb{F}_p)$ is cyclic of order ℓ for a 255-bit prime ℓ such that the embedding degree of E with respect to ℓ is 12. The curve E is ordinary and has endomorphism algebra $\mathbb{Q}(\sqrt{-3})$.

Miller's algorithm: We now describe Miller's algorithm which allows us to compute pairings *efficiently*. This elegant algorithm is the reason pairings are of practical value rather than purely of theoretical interest. A naive approach would mean $\mathbf{O}(\ell)$ operations in the elliptic curve over a finite field $\mathbb{F}_p$, which would be impractical when $\ell \approx 2^{256}$ and $p \approx 2^{381}$. Miller's algorithm allows us to compute the parings with $\mathbf{O}(\log(\ell))$ elliptic curve scalar multiplications and a final exponentiation in $\mathbb{F}_{q^k}^*$.

In practice, the best optimized Tate pairing is substantially faster than the best optimized Weil pairing. Hence, we typically use Tate pairings when the effective runtime is crucial, as is the case with blockchains.

As before, let P be a point on the elliptic curve E. The key ingredient is to determine a function f_P with divisor $\ell(P) - \ell(\infty_E)$. For every integer $i \geq 1$, the $f_{i,P}$ be a function whose divisor is

$$\mathrm{div}(f_i) = i(P) - ([i]P) - (i-1)(\infty_E).$$

In particular, $f_{1,P} = 1$ and $f_{\ell,P} = f_P$. The following relation enables efficient computation of $f_{\ell,P}(D_Q)$

Lemma 0.0.3. *Let $P \in E[\ell]$ and let i, j be integers ≥ 1. Let $\mathscr{L}_{[i]P,[j]P}$ be the line through $[i]P$ and $[j]P$. Let $\mathscr{V}_{[i+j]P}$ be the vertical line through $[i+j]P$. Then $f_{i+j,P} = f_{i,P} f_{j,P} \frac{\mathscr{L}_{[i]P,[j]P}}{\mathscr{V}_{[i+j]P}}$.*

It is important to note that the degree of $f_{n,P}$ grows linearly with n (en route to ℓ). Hence, the degree of the rational function $f_{n,P} \in \mathbb{F}_{q^k}(E)$ eventually becomes too large for $f_{n,P} \in \mathbb{F}_{q^k}(E)$ to be stored. Miller's algorithm circumvents this bottleneck by storing the evaluation $f_{n,P}(D_Q)$ at the divisor D_Q instead of storing $f_{n,P}$.

Miller's algorithm to compute the Tate pairing $T_\ell(P,Q)$

Input: $P \in E(\mathbb{F}_{q^k})[\ell]$; $Q = \widetilde{Q} + \ell \cdot E(\mathbb{F}_{q^k}) \in E(\mathbb{F}_{q^k})/\ell \cdot E(\mathbb{F}_{q^k})$;
$D_Q \sim (Q) - (\infty_E)$ with support disjoint from $(f_{\ell,P})$;
the binary representation $\ell = (r_{n-1} \cdots r_1 r_0)_2$ with $r_{n-1} = 1$

Output: $f_{\ell,P}(D_Q) \leftarrow f$

1. $R \leftarrow P$, $f \leftarrow 1$
2. **for** $i = n-2$ down to 0 do:
3. Compute the line functions $\mathscr{L}_{R,R}$ and $\mathscr{V}_{[2]R}$ for doubling R.

4. $R \leftarrow [2]R$

5. $f \leftarrow f^2 \cdot \frac{\mathscr{L}_{R,R}}{\mathscr{V}_{[2]R}}(D_Q)$

6. **if** $r_i = 1$ then

7. Compute the line functions $\mathscr{L}_{R,P}$ and $\mathscr{V}_{R+P}$ for adding R and P

8. $R \leftarrow R + P$

9. $f \leftarrow f \cdot \frac{\mathscr{L}_{R,P}}{\mathscr{V}_{R+P}}(D_Q)$

10. end **if**

11. end **for**

12. return $f^{(q^k-1)/\ell}$ □

Miller's algorithm to compute the Weil pairing has a similar structure. We can simulate Steps 1-11 to compute $f_{\ell,P}(D_Q)$, $g_{\ell,Q}(D_P))$ and then compute $\frac{f_{\ell,P}(D_Q)}{g_{\ell,Q}(D_P)} \in \mu_\ell(\mathbb{F}^*_{q^k})$.

0.0.4 Summary

There is consensus that type III pairings are faster than type I and type II pairings and that Tate pairings are faster than Weil pairings. Hence, it is optimal to use a Tate pairing for an ordinary pairing-friendly elliptic curve. The curve most suitable for this purpose seems to be the BLS12-381 curve.

The fundamental computation in elliptic curve cryptography is the scalar multiplication $m \cdot P$ for an integer m and an elliptic curve point P. This point is computed in runtime $\mathbf{O}(\log(m))$ via a sequence of point doublings and point additions. One of the components of a Tate pairing is the Miller loop, which is largely an extension of the scalar multiplication computation. The other key component in a Tate pairing is the final exponentiation which is a rather expensive exponentiation operation in a finite field of size q^k, where k is the embedding degree.

In pairing-based SNARKs such as PLONK, Groth16 etc, the Verifier's work is dominated by pairing computations. Thus, optimizing pairings is crucial for applications of SNARKs to blockchains.

0.0.5 Symbols

(f): divisor of a rational function $f \in \overline{\mathbb{F}}_p(E)$

∞_E: The E-point at infinity

D_P: the divisor $(P) - (\infty_E)$

$E(K)$: the group of K-valued points of E

$E[n]$: the n-torsion subgroup of E

$\mathscr{L}_{P,Q}$: $\begin{cases} \text{the line passing through } P \text{ and } Q \text{ if } P \neq Q \\ \text{the tangent line at } P \text{ if } P = Q \end{cases}$

$\mathscr{V}_P$: the vertical line passing through P (and $-P$)

$T_\ell(P,Q)$: the order ℓ reduced Tate pairing

$t_\ell(P,Q)$: the intermediate order ℓ Tate pairing

$w_\ell(P,Q)$: the order ℓ Weil pairing

BLS: Boneh-Lynn-Scott

$\mathrm{Div}(E)$: group of divisors on E

$\mathrm{Div}_F(E)$: group of divisors on E defined over F

$\mathrm{Div}^0(E)$: group of degree zero dvisors on E

$\mathrm{Div}^0_F(E)$: group of degree zero divisors on E defined over F

$\mathrm{ord}_P(f)$: the multiplicity of f at P on E

(E): The endomorphism ring of E

$^0(E)$: The endomorphism algebra of E

Gal_F: The absolute Galois group of F

$\mu_\ell(\mathbb{F}_{q^k})$: The ℓ-torsion of $\mathbb{F}^*_{q^k}$

$f_{n,P}$: A function with divisor $n(P) - ([n]P) - (n-1)(\infty_E)$ $(n \in \mathbb{Z}, P \in E(\mathbb{F}_{q^k}))$

$\mathrm{supp}(f)$: the support of a function f

$\Phi_k(X)$: The k-th cyclotomic polynomial