ELLIPTIC AND HYPERELLIPTIC CURVE CRYPTOGRAPHY

ANDREA MUNARO

Graduate Seminar

Contents

1. Elliptic Curves

Definition 1. Let k be a field. An *algebraic variety over k* is a k-scheme X such that there exists a covering by a finite number of affine open subschemes X_i which are affine varieties over k, i.e. each X_i is the affine scheme associated to a finitely generated algebra over k. A *projective variety over k* is a projective scheme over k, i.e. a k-scheme isomorphic to Proj $k[T_0, \dots, T_n]/I$ for a homogeneous ideal I of $k[T_0, \dots, T_n]$.

Note that projective varieties are algebraic varieties.

Definition 2. A *projective curve over k* is an irreducible projective variety over k of dimension one. An *elliptic curve over k* is a pair (E, O), where E is a smooth projective curve over k, geometrically irreducible (i.e. $E_{\bar{k}} = E \times_{\text{Spec } k} \bar{k}$ is irreducible), of genus $g = 1$, and $O \in E(k)$ is a k-rational point of E.

Recall that smoothness can be checked with the Jacobian criterion.

Remark 1. Let X be a k-scheme. For any affine open subset $U = \text{Spec } B$ we associate the quasi-coherent $\mathcal{O}_{X|U}$-module $\widetilde{\Omega_{B/k}}$, where $\Omega_{B/k}$ is the module of relative differential forms of B over k. Since it is compatible with localization [[11], 6.1.8], we can glue them into a quasi-coherent $\mathcal{O}_X$-module, called the *sheaf of relative differentials of* X and denoted by Ω_X. This turns out to be coherent and so by [[7], II.5.19] the following definition make sense.

Definition 3. For a smooth projective variety X over k, we define the genus of X to be $g(X) = \dim_k \Gamma(X, \Omega_X)$.

Definition 4. A scheme X is *regular in codimension one* if every local ring $\mathcal{O}_{X,x}$ of X of dimension one is regular.

Definition 5. Let X be a Noetherian integral separated scheme which is regular in codimension one. A *prime divisor* on X is a closed integral subscheme Y of codimension one. A *Weil divisor* is an element of the free abelian group $\text{Div}(X)$ generated by the prime divisors. Hence we can write a Weil divisor as a finite sum $D = \sum_i n_i Y_i$, where the Y_i are prime divisors and the n_i are integers. A divisor D is called *effective* if $n_i \geq 0$ for all i and it is denoted by $D \geq 0$.

From this we can put a partial ordering on $\mathrm{Div}(X)$: given $D, D' \in \mathrm{Div}(X)$ we write $D \geq D'$ if $D - D'$ is effective.

Note 1. *A projective curve X over k satisfies the assumptions in the previous Definition and so we can talk about divisors on it. In this case a prime divisor is just a closed point. Therefore an arbitrary divisor can be written as $D = \sum_x n_x \cdot x$, where the x are closed points and $n_x \in \mathbb{Z}$.*

Definition 6. The *degree of D* is $\deg(D) = \sum n_x \cdot \dim_k k(x)$, where $k(x)$ is the residue field at the closed point x.

The above Definition gives rise to a $\mathbb{Z}$-module morphism $\deg : \mathrm{Div}(X) \longrightarrow \mathbb{Z}$. The kernel is a subgroup of $\mathrm{Div}(X)$ denoted by $\mathrm{Div}^0(X)$. Since a principal divisor on a smooth projective curve over k has degree 0 [[7], II.6.10], we can define the quotient group $\mathrm{Cl}^0(X)$ of $\mathrm{Div}^0(X)$ by the subgroup of principal divisor on X.

Remark 2. Let Y be a prime divisor on X and $\xi \in Y$ its generic point. Then $\dim \mathcal{O}_{X,\xi} = \mathrm{codim}(\overline{\{\xi\}}, X) = \mathrm{codim}(Y, X) = 1$ [[11], Exercise 2.5.2] and so the local ring $\mathcal{O}_{X,\xi}$ is regular by the assumptions on X. Thus, it is a discrete valuation ring. Furthermore, the quotient field of $\mathcal{O}_{X,\xi}$ is the function field $k(X)$ of X. Denote the corresponding discrete valuation by v_Y. If $f \in k(X)^*$ then $v_Y(f) \in \mathbb{Z}$. If it is positive, we say f has a *zero along* Y of order $v_Y(f)$ and if it is negative, we say f has a *pole along* Y of order $-v_Y(f)$.

At this point we can define the divisor of a function.

Definition 7. Let $f \in k(X)^*$. The *divisor of f* is $(f) = \sum v_Y(f) \cdot Y$, where the sum is taken over all prime divisors of X. This is a finite sum [[7], II.6.1] and therefore (f) is well-defined. Any divisor which is equal to the divisor of a rational function is called a *principal divisor*.

Note that if $f, g \in k(X)^*$, then $(f/g) = (f) - (g)$. Therefore sending a function to its divisor is a homomorphism from the multiplicative group $k(X)^*$ to the additive group $\mathrm{Div}(X)$. Its image, which consists of the principal divisors, is a subgroup of $\mathrm{Div}(X)$. The corresponding quotient group is called the *divisor class group of* X and denoted by $\mathrm{Cl}(X)$. Two divisors D, D' are called *linearly equivalent*, written $D \sim D'$, if $D - D'$ is a principal divisor.

Divisors on a projective curve X over k are interesting for us because, by the following theorem, they correspond to invertible sheaves on X, i.e. locally free sheaves of $\mathcal{O}_X$-modules of rank one. Isomorphism classes of invertible sheaves on X form an abelian group under tensor product called the Picard group of X, $\mathrm{Pic}(X)$.

Proposition 1. *Let X be a projective variety over k. Then there is a natural isomorphism $Cl(X) \cong Pic(X)$.*

Proof. See [[7], II.6.16]. □

For any divisor $D \in \mathrm{Div}(X)$ define $L(D) = \{f \in k(X)^* : D + (f) \geq 0\} \cup \{0\}$ (this is nothing but the set of global sections $\Gamma(X, \mathcal{L}(D))$ of the invertible sheaf associated to D). This is a finite dimensional k-vector space and so let $\ell(D) = \dim_k L(D)$. The module $\Omega_{k(X)/k}$ of relative differential forms of $k(X)$ over k is in fact a one dimensional $k(X)$-vector space [[11], 6.1.15 and 3.2.15]. For $f \in k(X)$ we have that df is a basis of $\Omega_{k(X)/k}$ over $k(X)$ if and only if $k(X)/k(f)$ is a finite separable extension [[11], 6.1.16]. Let $x \in X$ be a point on the projective curve X and let $f \in k(X)^*$ be an uniformizing element at x, i.e. such that $v_x(f) = 1$. Then by [[14], II.1.4], for every $\omega \in \Omega_{k(X)/k}$ there exists a unique $g \in k(X)$ such that $\omega = gdf$, denoted by ω/df. For $0 \neq \omega \in \Omega_{k(X)/k}$ the quantity $v_x(\omega/df)$ is independent of the choice of the uniformizing element f [[14], II.4.3(c)]. It is called the *order of ω at x* and denoted by $\mathrm{ord}_x(\omega)$. Furthermore $\mathrm{ord}_x(\omega) = 0$ for all but finitely many $x \in X$ [[14], II.4.3(e)]. Then we can associate a divisor to $0 \neq \omega \in \Omega_{k(X)/k}$ by setting $\mathrm{div}(\omega) = \sum_x \mathrm{ord}_x(\omega) \cdot x$, where the sum is taken over the closed points $x \in X$. If $\omega' \in \Omega_{k(X)/k}$ is another differential then $\omega' = f\omega$ for some $f \in k(X)^*$ and so we have $\operatorname{div}(\omega') = (f) + \operatorname{div}(\omega)$. Then any divisor linearly equivalent to $\operatorname{div}(\omega)$ is called a *canonical divisor*.

Note that if $\deg(D) < 0$ then $L(D) = \{0\}$.

Theorem 1 (Riemann-Roch). *Let X be a smooth projective curve over k of genus g and let K be a canonical divisor on X. Then*

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g.$$

Proof. See [[7], IV.1.3] or [[11], 7.3.33]. □

Corollary 1. *Let X be a smooth projective curve over k of genus g and let K be a canonical divisor on X. Then*
(1) $\deg(K) = 2g - 2$.
(2) Let D be a divisor on X. If $\deg(D) > 2g - 2$, *then* $\ell(D) = \deg(D) - g + 1$.

Proof. (1). Taking $D = K$ in Riemann-Roch, we get $\ell(K) - \ell(0) = \deg(K) + 1 - g$. Since $g = \ell(K)$ and $\ell(0) = 1$ we are done.
(2). By assumption and using (1) we have $\deg(K - D) < 0$. Hence $\ell(K - D) = 0$. Therefore, applying Riemann-Roch we have $\ell(D) - 0 = \deg(D) + 1 - g$. □

Using Riemann-Roch one can prove the following remarkable proposition which says that elliptic curves are given by "nice" cubic equations.

Proposition 2. *Let (E, O) be an elliptic curve over k. Then there exists an isomorphism $\phi : E \longrightarrow C$, where C is the smooth projective curve given by a Weierstrass equation*

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \subset \mathbb{P}^2_k, \tag{1.1}$$

for some $a_i \in k$, satisfying $\phi(O) = [0 : 1 : 0]$.
Conversely if C is given by 1.1 and smooth, then $(C, [0 : 1 : 0])$ is an elliptic curve over k.

Proof. See [[14], III.3.1]. □

Given a projective cubic curve as in 1.1, equipped with the point $O = [0 : 1 : 0]$ at infinity, and a projective line, we know by Bezout's Theorem that they intersect in exactly three points counted with multiplicities. Then we can define a composition law $\oplus$ in the following way: let $P, Q \in C$ and let L be the line through P and Q (if $P = Q$, let L be the tangent line to C at P), and let R be the third point of intersection of L with C. Let L' be the line through R and O. Then L' intersects C at R, O, and a third point. We define that third point to be $P \oplus Q$. It is not clear a priori that this composition law makes C into an abelian group with identity element O. But this is the case, even though proving associativity involves cumbersome calculations.

On the other hand considering our definition of elliptic curve we can put a group structure on it in a natural way and this is in fact the reason why the composition law $\oplus$ is a group law.

Proposition 3. *Let (E, O) be an elliptic curve over k. Then the map $E_0 \longrightarrow Cl^0(E)$, where E_0 is the set of closed points on E, which sends a closed point P to the class of $P - O$ is bijective.*

Proof. Let $D \in \operatorname{Div}^0(E)$. Since $\deg(D - O) = 1 > 0$, by Corollary 1 (2), we have $\ell(D + O) = \deg(D + O) + 1 - 1 = 1$. Now, any $f \in k(X)^*$ is a basis for the one dimensional vector space $L(D + O)$. Since $(f) + D + O \geq 0$ and $\deg((f)) = 0$ we have $(f) = -D - O + P$, for some closed point P. Hence there exists a point P such that $D \sim P - O$. In fact it is unique. If P' is another point with the same property then $P - O \sim D \sim P' - O$. Choose $t \in k(X)^*$ such that $(t) = P - O - (P' - O)$. Then $t \in L(P' - O)$. By Riemann-Roch we have $\ell(Q) = \deg(Q) = 1$, but the costant functions are already in $L(Q)$ and so we must have $L(Q) = k$ and $t \in k$. Hence $P = P'$. Now define a map σ from $\operatorname{Div}^0(E)$ to the set of closed points of E by the association described above. Clearly it is surjective since $\sigma(P - O) = P$. Suppose further that $\sigma(D_i) = P_i - O$ for closed points P_i, $i = 1, 2$. Then

$$D_1 \sim D_2 \Leftrightarrow P_1 - O \sim P_2 - O \Leftrightarrow P_1 \sim P_2 \Leftrightarrow P_1 = P_2 \Leftrightarrow \sigma(D_1) = \sigma(D_2).$$

Therefore we have the desired bijection with inverse given by $\kappa : P \mapsto [P - O]$. □

Since Cl^0 is a group we can just put its group structure on the set of closed points E_0, making it into an abstract group. Furthermore one can prove that the two group laws defined above are the same [[14], III.3.4(e)] and that (E, O) is an abelian variety over k, i.e. the group composition law defines morphisms $+ : E \times E \longrightarrow E$, $(P_1, P_2) \mapsto P_1 + P_2$ and $- : E \longrightarrow E$, $P \mapsto -P$ [[14], III.3.6].

Note 2. *If k is algebraically closed and X is a k-scheme locally of finite type, then the closed points are precisely the k-rational points [[1], I.6.5.3]. In particular we have a group structure on $E(k)$. If k is not algebraically closed just restrict the group structure on $E(\bar{k})$ to $E(k)$.*

Corollary 2. *Let (E, O) be an elliptic curve over k, and let $D = \sum n_P P \in Div(E)$. Then D is a principal divisor if and only if $\deg(D) = 0$ and $\sum [n_P]P = O$, where the second sum is addition on E.*

Proof. We know that the degree of a principal divisor is 0. Now let $D \in \mathrm{Div}^0(E)$ and let σ as in the Proposition above. Then

$$D \text{ principal} \Leftrightarrow D \sim 0 \Leftrightarrow \sigma(D) = O \Leftrightarrow \sum [n_P]\sigma((P) - (O)) = O \Leftrightarrow \sum [n_P]P = O.$$

□

Using non-homogeneous coordinates we can think of an elliptic curve over k as the set of solutions of a Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with $a_i \in k$, plus the extra point $O = [0 : 1 : 0]$ at infinity. Note that given points $P_i = (x_i, y_i) \in E$ we can find explicit formulas for the group law [[14], III.2.3].

For an elliptic curve $(E, \mathbb{F}_q)$ over a finite field we have a trivial upper bound $|E(\mathbb{F}_q)| \leq 2q + 1$. Heuristically, we might expect a random quadratic equation to have a solution with probability 1/2. Thus, perhaps $|E(\mathbb{F}_q)| \sim q + 1$. In fact by a remarkable result of Hasse we have $||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$ [[14], V.1.1]. In 1985 Schoof [16] proposed a polynomial time algorithm that computes $|E(\mathbb{F}_q)|$ in $O((\log q)^8)$ steps. It was further improved, with complexity $O((\log q)^6)$, by Schoof, Elkies and Atkin, taking the name of SEA algorithm.

1.1. Weil pairing.

Definition 8. Let (E, O) and (E', O') be elliptic curves over k. Then an *isogeny* is a morphism of curves over k, $\phi : E \longrightarrow E'$, satisfying $\phi(O) = O'$.

Remark 3. Let X, Y be smooth projective curves over k and let $f : X \longrightarrow Y$ be a morphism. Then either $f(X)$ consists of one point, or $f(X) = Y$. In the latter case, f is a finite morphism and $k(X)$ is a finite field extension of $k(Y)$ [[7], II.6.8]. Then we define the *degree of f* to be $\deg(f) = [k(X) : k(Y)]$.

The Remark above tells us that, except for the zero isogeny, defined by $[0](P) = O$ for all $P \in E$, every other morphism is a finite morphism and we can talk about its degree. By definition we set $\deg([0]) = 0$. It is easy to see that the multiplication by n map $[n] : E \longrightarrow E$, defined in the natural way for every $n \in \mathbb{Z}$, is in fact an isogeny. It is non-constant if $n \neq 0$ [[14], III.4.2].

Let (E, O) be an elliptic curve over k, and let $n \geq 2$ be an integer coprime to $\mathrm{char}(k)$ (no restriction if $\mathrm{char}(k) = 0$). We know that the n-torsion group $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ [[14], III.6.4], thus it is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank two and we want to define a bilinear pairing

$$e_n : E[n] \times E[n] \longrightarrow \mu_n,$$

where we denote by μ_n the group of n-th roots of unity.

The divisor $D = n(T) - n(O)$ is principal by Corollary 2, and so there exists $f \in k(E)^*$ such that $(f) = D$. Since the multiplication by n isogeny $[n]$ is non-costant, then it is surjective. Therefore let $T' \in E$ such that $[n](T') = T$. Note that the divisor

$$D' = \sum_{P \in E[n]} ((T' + P) - (P))$$

is independent of the choice of T'. Clearly it has degree 0 and since $|E[n]| = n^2$, we have

$$\sum_{P \in E[n]} (T' + P - P) = \sum_{P \in E[n]} T' = [n^2]T' = [n]T = O.$$

Again by Corollary 2, $D' = (g)$ for some $g \in k(E)^*$. On the other hand

$$(g^n) = n(g) = \sum_{P \in E[n]} (n(T' + P) - n(P))$$

and

$$([n]^* f) = \sum_{P \in E[n]} (n(T' + P) - n(P)).$$

Then $(g^n/[n]^* f) = 0$. But the only rational functions without poles or zeros are the constant functions and so $g^n = \lambda [n]^* f$, for some $\lambda \in k^*$. Therefore, replacing f by λf, (f) doesn't change and we may assume $g^n = [n]^* f$. Note that the map $\tau_S : E \longrightarrow E$, $R \mapsto R + S$ is clearly an isomorphism for every $S \in E$. Now let $S \in E[n]$ be another n-torsion point. We have $(g \circ \tau_S)^n = f \circ [n] \circ \tau_S = f \circ [n] = g^n$ and so we define

$$e_n(S, T) = \frac{g \circ \tau_S}{g} \in \mu_n.$$

Note that by the considerations above it is well defined.

Proposition 4. *The pairing e_n is called the **Weil pairing**. It is bilinear, alternating, nondegenerate. Furthermore it is Galois invariant if k is perfect.*

Proof. Linearity in the first factor is immediate: for $S, S', T \in E[n]$,

$$e_n(S + S', T) = \frac{g \circ \tau_{S+S'}}{g} = \frac{g \circ \tau_{S+S'}}{g \circ \tau_S} \frac{g \circ \tau_S}{g} = e_n(S, T) e_n(S', T).$$

See [[14], III.8.1] for the remaining assertions. □

Corollary 3. *Let $\{T_1, T_2\}$ be a basis of $E[n]$. Then $e_n(T_1, T_2)$ is a primitive n-th root of unity.*

Proof. Suppose $e_n(T_1, T_2) = \zeta$ with $\zeta^d = 1$ for some $d \leq n$. Then $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$. Now let $S \in E[n]$. Then $S = aT_1 + bT_2$ for some $a, b \in \mathbb{Z}$. Therefore,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

But since this holds for all S, then $dT_2 = O$. Hence $d = n$. □

2. Elliptic Curve Cryptography

The earliest public-key cryptosystems, introduced for the first time by Diffie and Hellman in 1976, were based on the apparent intractability of the discrete logarithm problem (DLP) for the multiplicative group $\mathbb{F}_q^*$ of a finite field. In 1985, Miller and Koblitz proposed, independently, to use the group of points of an elliptic curve defined over a large finite field, and later Koblitz suggested to use the group of points of the Jacobian of a hyperelliptic curve defined over a finite field. The reason for considering other groups was the existence of subexponential-time algorithms (the most efficient attack is the Index Calculus) capable to find discrete logs in finite fields. On the other hand, under certain conditions, there is no practical Index Calculus method known to solve the DLP in the elliptic and hyperelliptic case and it seems that for both theoretical and practical reasons such a method doesn't exist [18]. In fact for the elliptic curve discrete logarithm problem (ECDLP) the only known algorithms are generic, i.e. they work for arbitrary groups, regardless of their structure. In this class, besides the naive algorithm for solving the DLP, which takes $O(n)$ steps and requires $O(1)$ storage, we have basically other two algorithms:

- The Shanks' baby-step giant-step basically computes two lists of elements and compares them to see if there is a match. It solves the DLP in $O(\sqrt{n})$ steps with $O(\sqrt{n})$ storage.
- The Pollard's ρ algorithm relies on the so called "birthday paradox": if we compute approximately $\sqrt{n}$ random powers, there is a good chance that two of them will be the same. Its running time is $O(\sqrt{n})$ and it has no storage requirements.

On the other hand the Pohlig-Hellman algorithm reduces the DLP for elements of arbitrary order to the DLP for elements of prime order. If the order of the group is $N = \prod p_i^{e_i}$, it has running time $O(\sum e_i(\log N + \sqrt{p_i}))$. Hence the DLP is not secure if the order of the group is a product of powers of small primes. In 1997 Shoup [17] proved that any algorithm that solves the DLP in every group takes on average at least $\Omega(\sqrt{n})$ steps.

2.1. MOV algorithm.

Definition 9. Let $\mathbb{F}_q$ be a finite field and let $N \geq 1$ be an integer. The embedding degree of N in $E(\mathbb{F}_q)$ is the smallest integer $d \geq 1$ such that $\mu_N \subset \mathbb{F}_{q^d}^*$, i.e. the smallest integer satisfying $q^d \equiv 1 \pmod{N}$.

Proposition 5 (MOV Algorithm, [12])**.** *Let $E/\mathbb{F}_q$ be an elliptic curve, let $P, Q \in E(\mathbb{F}_q)$ be points with P of prime order N, and let d be the embedding degree of N in $\mathbb{F}_q$. Assume that* $\gcd(q, N) = 1$. *Then there is a polynomial-time algorithm that reduces the ECDLP for P and Q to the DLP in $\mathbb{F}_{q^d}^*$.*

Proof. We are looking for an integer m such that $Q = [m]P$. Choose a point $T \in E[N]$ such that $\{P, T\}$ is a basis for $E[N]$. By Corollary 3 we have that $e_N(P, T)$ is a primitive N-th root of unity, and so by definition of embedding degree $e_N(P, T) \in \mathbb{F}_{q^d}^*$. On the other hand by linearity of the Weil pairing we have $e_N(Q, T) = e_N([m]P, T) = e_N(P, T)^m$. Since we know the values of P, Q, T we can solve the DLP $e_N(Q, T) = e_N(P, T)^m$ in $\mathbb{F}_{q^d}^*$. The only computations involved are the search for the point T and the calculations of the pairing values $e_N(Q, T)$ and $e_N(P, T)$. For the Weil pairing computations there is a linear-time algoritm by Miller [[14], XI.8]. We will prove below that, under a further assumption on N, we have $E[N] \subset E(\mathbb{F}_{q^d})$, and so all the computations may be done in $\mathbb{F}_{q^d}$. To construct $T \in E(\mathbb{F}_{q^d})$, we randomly choose points $T \in E(\mathbb{F}_{q^d})$ of order N until we find one such that $e_N(P, T)$ is a primitive N-th root of unity. □

Lemma 1. *Let $E/\mathbb{F}_q$ be an elliptic curve, let $N \geq 1$ be an integer satisfying* $\gcd(q-1, N) = 1$, *and let d be the embedding degree of N in $\mathbb{F}_q$. Suppose that $E(\mathbb{F}_q)$ contains a point of order N. Then $E[N] \subset E(\mathbb{F}_{q^d})$.*

Proof. Let $P \in E(\mathbb{F}_q)$ be the point of order N, and choose a point $T \in E[N]$ such that $\{P, T\}$ is a basis for $E[N]$. Let $\phi \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ be the Frobenius endomorphism. We have $P^\phi = P$ and $T^\phi = [a]P + [b]T$ for some $a, b \in \mathbb{Z}/N\mathbb{Z}$. By Proposition 4 we have

$$e_N(P, T)^q = e_N(P, T)^\phi = e_N(P^\phi, T^\phi) = e_N(P, [a]P + [b]T) = e_N(P, P)^\phi e_N(P, T)^b = e_N(P, T)^b.$$

Since $e_N(P, T)$ is a primitive N-th root of unity we have $b \equiv q \pmod{N}$ and so $T^\phi = [a]P + [q]T$. Applying ϕ repeatedly to T and using the fact that ϕ fixes P we get

$$T^{\phi^d} = [a(1 + q + \cdots + q^{d-1})]P + [q^d]T.$$

By definition of embedding degree we have $q^d \equiv 1 \pmod{N}$. Hence $[q^d]T = T$. By assumption $\gcd(q-1, N) = 1$, and so $1 + q + \cdots + q^{d-1} \equiv 0 \pmod{N}$. Therefore $[1 + q + \cdots + q^{d-1}]P = O$ and $T^{\phi^d} = T$, which implies that $T \in E(\mathbb{F}_{q^d})$. □

Definition 10. Let $E/\mathbb{F}_q$ be an elliptic curve, where q is a power of the prime number p. Then $|E(\mathbb{F}_q)| = q + 1 - a$ for some integer a. The curve E is called *supersingular* if $a \equiv 0 \pmod{p}$.

Proposition 6. *Let $p \geq 5$ be a prime and let $E/\mathbb{F}_p$ be an elliptic curve. Then E is supersingular if and only if $a = 0$, i.e. $|E(\mathbb{F}_p)| = p + 1$.*

Proof. One direction is clear. If $E/\mathbb{F}_p$ is supersingular, then by Hasse's Theorem and since $p \geq 5$, we have

$$|a| = ||E(\mathbb{F}_p)| - p - 1| \leq 2\sqrt{p} < p.$$

Therefore $a \equiv 0 \pmod{p}$ implies $a = 0$. □

For supersingular curves we have $d \leq 6$ [12], and usually $d = 2$. Indeed, if $p \geq 5$ and $P \in E(\mathbb{F}_p)$ is a point of order N then $p \equiv -1 \pmod{N}$. Hence $p^2 \equiv 1 \pmod{N}$ and so N has embedding degree 2 in $\mathbb{F}_p$. Therefore, by the MOV Algorithm, discrete logarithms can be computed more easily for these curves than for arbitrary elliptic curves. The general rule is then to avoid supersingular elliptic curves for traditional cryptographic applications. This is unfortunate, since an attractive feature of supersingular curves is that calculations can often be done quickly on them.

The reason the MOV attack works is that it is possible to use the Weil pairing. Then, in order to avoid this, it was suggested to use elliptic curves $E/\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = q$, called *anomalous*. However, it turns out that there is a different attack for anomalous curves proposed indipendently by Semaev, Smart, Satoh and Araki in 1998, that works even faster for these curves than the MOV attack works for supersingular curves [[14], XI.6.5].

2.2. **Selecting an Appropriate Elliptic Curve.** The following are the security requirements for cryptographic applications of the Mordell-Weil group $E(\mathbb{F}_q)$ involving the ECDLP. Let N be the largest prime divisor of $|E(\mathbb{F}_q)|$.

- To resist the combination of Pohlig-Hellman and Pollard ρ attacks, the Mordell-Weil group should have order almost prime, i.e. $|E(\mathbb{F}_q)|/N \leq 4$.

- The embedding degree of N in $E(\mathbb{F}_q)$ should be $d > 20$, in order to avoid the MOV attack.

- To avoid Semaev-Smart-Satoh-Araki attack, $|E(\mathbb{F}_q)|$ should not be equal to q.

Note that we can use the SEA algorithm to calculate $|E(\mathbb{F}_q)|$. In the following we present four techniques for selecting an appropriate elliptic curve.

- *Using Hasse's Theorem.* An elliptic curve $E/\mathbb{F}_q$ can be viewed as an elliptic curve over any extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is a subgroup of $E(\mathbb{F}_{q^k})$. Let $a = q + 1 - |E(\mathbb{F}_q)|$. Then $\left|E(\mathbb{F}_{q^k})\right| = q^k + 1 - \alpha^k - \beta^k$, where α and β are the complex roots of $T^2 - aT + q$ [[14], V.2.3.1]. This technique can be used to choose curves over $\mathbb{F}_{2^m}$ where m is divisible by a small integer $l \geq 1$. We first pick an elliptic curve over over a small field $\mathbb{F}_{2^l}$, compute $|E(\mathbb{F}_{2^l})|$ and determine $|E(\mathbb{F}_{2^m})|$ as above. If the three security requirements are not satisfied, another curve is selected and the process repeated. Note that since the number of elliptic curves over $\mathbb{F}_{2^l}$ is relativeley small, for a fixed m it may not be possible to construct an appropriate curve using this method.

- *The Global Method.* We can choose an elliptic curve defined over a number field and then reduce it modulo a prime ideal in order to obtain an elliptic curve defined over a finite field satisfying the three security requirements. For instance, we can start with $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Q}$, and reduce it modulo p for large primes, where p doesn't divide the discriminant of E, in a way that the number N_p of points on the curve over $\mathbb{F}_p$ is a prime or a prime times a small factor.

  Koblitz conjectured the following in 1988. Denote by $E_p(\mathbb{F}_p)$ the reduction of E modulo p. If $E/\mathbb{Q}$ is an elliptic curve without complex multiplication and which is not isogenous to a curve with non-trivial rational torsion, then

$$|\{p \leq x : p \text{ has good reduction}, |E_p(\mathbb{F}_p)| \text{ is prime}\}| \sim C_E \frac{x}{(\log x)^2}$$

  as $x \longrightarrow \infty$, where C_E is an explicit constant. The problem is still open but was shown to be true on average over a familiy of elliptic curves by Balog, Cojocaru and David [2]. Furthermore, Cojocaru proved in 2005 [6] that if E is a complex multiplication curve not isogenous to a curve with non-trivial rational torsion then

$$|\{p \leq x : p \text{ has good reduction, } |E_p(\mathbb{F}_p)| \text{ has at most 5 prime factors}\}| \geq C_E \frac{x}{(\log x)^2}$$

as $x \longrightarrow \infty$, where C_E is a positive constant. Similar results were obtained by Steuding and Weng for non CM curves assuming the Generalized Riemann hypothesis.

- *The Complex Multiplication Method.* The method of complex multiplication (CM) allows the choice of an elliptic curve order before the curve is explicitly constructed. Thus orders can be generated and tested to satisfy the security requirements and a curve is constructed when these conditions are met. Let p be a prime such that $4p = Dy^2 + a^2$, where $D > 0, y$ and a are integers. Class field theory of imaginary quadratic fields tells us that given D, one can construct the Hilbert class polynomial $H_D(X)$, of degree $h(-D)$ (the class number of $\mathbb{Q}(\sqrt{-D})$, the roots of which generate the maximal abelian unramified extension, i.e. class field, of $\mathbb{Q}(\sqrt{-D})$. Moreover, this polynomial splits on $\mathbb{F}_p$ as a product of linear factors, and its roots are the j-invariants of elliptic curves E with $|E(\mathbb{F}_p)| = p + 1 - a$. This method works when $h(-D)$ is small.
- *Choosing a curve at random.* We can select random parameters $a, b \in \mathbb{F}_q$, calculate $|E(\mathbb{F}_q)|$, and repeat the process until the security requirements are satisfied.

A general philosophy in cryptography is that, whenever possible, parameters should be chosen by some random process. If a special choice is made to increase efficiency, there is always the risk that the same property that made the choice so attractive will also lead to vulnerability to an unanticipated attack.

2.3. **Modified Weil Pairing.** In cryptographic applications we generally want to evaluate the pairing at points aP and bP for some integers a, b. But since the Weil pairing is alternating we have $e_n(aP, bP) = e_n(P, P)^{ab} = 1$ and this is not helpful.

Definition 11. Let $\ell \geq 3$ be a prime, let E be an elliptic curve, let $P \in E[\ell]$ be a point of order ℓ, and let $\phi : E \longrightarrow E$ be a map. ϕ is called an *ℓ-distortion map for P* if it has the following properties:
(i) $\phi(nP) = n\phi(P)$ for all $n \geq 1$.
(ii) $e_\ell(P, \phi(P))$ is a primitive ℓ-th root of unity.

Proposition 7. *Let E be an elliptic curve, let $\ell \geq 3$ be a prime, and let $P, Q \in E[\ell]$. Then the following are equivalent:*
(a) $\{P, Q\}$ is a basis for $E[\ell]$.
(b) $P \neq O$ and Q is not a multiple of P.
(c) $e_\ell(P, Q)$ is a primitive ℓ-th root of unity.
(d) $e_\ell(P, Q) \neq 1$.

Proof. Clearly (a) implies (b). Conversely, suppose that (a) is false, i.e. $uP + vQ = O$ for some $u, v \in \mathbb{Z}/\ell\mathbb{Z}$ not both zero. If $v = 0$ then $P = O$ and so (b) is false. If $v \neq 0$, then v has an inverse in $\mathbb{Z}/\ell\mathbb{Z}$, so $Q = -v^{-1}uP$ is a multiple of P, and (b) is false. Then (a) and (b) are equivalent. Let $r \geq 1$ be the order of $e_\ell(P, Q)$. Then

$$e_\ell(P, Q)^{\gcd(r,\ell)} = e_\ell(P, Q)^{sr+t\ell} = (e_\ell(P, Q)^r)^s (e_\ell(P, Q)^\ell)^t = 1,$$

for some $s, t \in \mathbb{Z}$. Then $r = \gcd(r, \ell)$, so $r \mid \ell$. Since ℓ is prime, it follows that either $r = 1$, so $e_\ell(P, Q) = 1$, or else $r = \ell$. Then (c) and (d) are equivalent.
Suppose (a) holds. Then $P \neq O$ and by nondegeneracy of the Weil pairing there exists $R \in E[\ell]$ with $e_\ell(P, R) \neq 1$. On the other hand we have $R = uP + vQ$, for some $u, v \in \mathbb{Z}/\ell\mathbb{Z}$. Then

$$1 \neq e_\ell(P, R) = e_\ell(P, uP + vQ) = e_\ell(P, P)^u e_\ell(P, Q)^v = e_\ell(P, Q)^v.$$

Hence $e_\ell(P, Q) \neq 1$, and (d) is true.
Finally we prove that (d) implies (b). Suppose (b) is false. Then either $P = O$ or $Q = uP$, for some $u \in \mathbb{Z}/\ell\mathbb{Z}$. But if $P = O$, then $e_\ell(P, Q) = e_\ell(O, Q) = 1$, while if $Q = uP$, then

$$e_\ell(P, Q) = e_\ell(P, uP) = e_\ell(P, P)^u = 1.$$

In both cases $e_\ell(P, Q) = 1$ and so (d) is false.

Alternatively, we could have proved (a) equivalent to (c). Indeed, (a) implies (c) is just Corollary 3. For the reverse implication, suppose (a) is false. Then with notation as above we have two cases. If $v = 0$, then $P = O$, and so $e_\ell(P, Q) = e_\ell(O, Q) = 1$ is not a primitive ℓ-th root of unity. If $v \neq 0$, then $Q = -v^{-1}uP$, and again $e_\ell(P, Q) = e_\ell(P, -v^{-1}uP) = e_\ell(P, P)^{-v^{-1}u} = 1$, showing that (c) is false. □

Definition 12. Let E be an elliptic curve, let $P \in E[\ell]$, and let ϕ be an ℓ-distortion map for P. The *modified Weil pairing* $\hat{e}_\ell$ on $E[\ell]$ (relative to ϕ) is defined by $\hat{e}_\ell(Q, Q') = e_\ell(Q, \phi(Q'))$.

The modified Weil pairing is nondegenerate in the following sense.

Proposition 8. *Let E be an elliptic curve, let $P \in E[\ell]$, and let Q, Q' be multiples of P. Then $\hat{e}_\ell(Q, Q') = 1$ if and only if $Q = O$ or $Q' = O$*

Proof. Let $Q = sP$ and $Q' = tP$. Then we have

$$\hat{e}_\ell(Q, Q') = \hat{e}_\ell(sP, tP) = e_\ell(sP, \phi(tP)) = e_\ell(sP, t\phi(P)) = e_\ell(P, \phi(P))^{st}.$$

But $e_\ell(P, \phi(P))$ is a primitive ℓ-th root of unity and so

$$\hat{e}_\ell(Q, Q') \iff \ell \mid st \iff \ell \mid s \text{ or } \ell \mid t \iff Q = O \text{ or } Q' = O.$$

□

We need to give an example of an elliptic curve with a distortion map. For this purpose we'll consider the elliptic curve $E : y^2 = x^3 + x$ defined over $\mathbb{F}_p$, with $p \equiv 3 \pmod 4$. We can check that this is a supersingular elliptic curve [[14], V.4.5].

Proposition 9. *Let E be the elliptic curve $E : y^2 = x^3 + x$ over k and suppose that there exists $\alpha \in k$ such that $\alpha^2 = -1$. Define a map ϕ by $\phi(x, y) = (-x, \alpha y)$ and $\phi(O) = O$. Then ϕ is an isogeny. In particular $\phi(nP) = n\phi(P)$ for all $n \geq 1$ and $P \in E(k)$.*

Proof. See [[14], III.4.8] and [[8], 5.51]. □

Proposition 10. *Fix the following quantities:*

- *A prime p satisfying $p \equiv 3 \pmod 4$.*
- *The elliptic curve $E : y^2 = x^3 + x$.*
- *An element $\alpha \in \mathbb{F}_{p^2}$ satisfying $\alpha^2 = -1$.*
- *The map $\phi(x, y) = (-x, \alpha y)$.*
- *A prime $\ell \geq 3$ such that there exists a nonzero point $P \in E(\mathbb{F}_p)[\ell]$.*

Then ϕ is an ℓ-torsion map for P.

Proof. By the quadratic reciprocity, $\mathbb{F}_p$ does not contain an element satisfying $\alpha^2 = -1$. However $\mathbb{F}_{p^2}$ contains a square root of -1, since if g is a primitive root for $\mathbb{F}_{p^2}^*$, then $\alpha = g^{(p^2-1)/4}$ satisfies $\alpha^4 = 1$ and $\alpha^2 \neq 1$, so $\alpha^2 = -1$. Since P is a point of order ℓ, by the Proposition above we have $\ell\phi(P) = \phi(\ell P) = \phi(O) = O$, and so $\phi(P) \in E[\ell]$. In view of Proposition 7 suppose that $\phi(P)$ is a multiple of $P = (x, y) \in E(\mathbb{F}_p)$. The coordinates of P are in $\mathbb{F}_p$ and so the coordinates of $\phi(P) = (-x, \alpha y)$ are also in $\mathbb{F}_p$. But $\alpha \notin \mathbb{F}_p$ and we must have $y = 0$. But $P = (x, 0)$ is a point of order 2, contradicting the fact that P has order $\ell \geq 3$. □

2.4. **Applications of the Weil Pairing.** In the previous section we described a negative application of the Weil pairing, namely the MOV attack which reduces the ECDLP to the DLP in the multiplicative group of a finite field. In this section we describe three positive applications of the Weil pairing. The first is a version of the Diffie-Hellman key exchange involving three people, the second is an ID-based public key cryptosystem in which the public keys can be selected by their owners and the third is a digital signature scheme which gives signatures that are half the size of those produced by DSA. The elliptic curves used in the practical implementation of the following examples are mostly supersingular elliptic curves. At first it might seem strange to use elliptic curves which are known to be weaker than random curves. However, it is known that distortion maps exist on supersingular elliptic curves and that distortion maps that do not commute with the Frobenius endomorphism do not exist on ordinary elliptic curves [19]. Hence supersingular elliptic curves are good candidates provided we choose a large prime p, since they are well known and very easy to build.

2.5. **Tripartite Diffie-Hellman Key Exchange.** We know the classical Diffie-Hellman key exchange in which two people with no prior knowledge of each other, jointly establish a shared secret key over an insecure communications channel. Let's recall briefly the procedure.
The following are publicly known system parameters: a group G and an element $P \in G$ of order p, usually taken as an integer divisible by a large prime due to the Pohlig-Hellman algorithm. Alice selects a random integer $a \in [1, p-1]$ and computes $A = aP \in G$. Bob selects a random integer $b \in [1, p-1]$ and computes $B = bP \in G$. Alice and Bob exchange the values of A and B over the channel monitored by an eavesdropper Eve. Then Alice computes aB and Bob computes bA. In this way they have shared the value abP. Eve is faced with the task of computing abP given P, aP and bP. This is known as the *Diffie-Hellman problem* and at present the only way known to solve it is to solve the associated DLP, i.e. to compute a and b. the Diffie-Hellman protocol can be viewed as a one-round protocol because the two exchanged messages are independent of each other and it can be extended in an obvious way to three people, obtaining a two-rounds protocol. A natural question is to ask whether there exists a three-people one-round key exchange protocol secure against eavesdroppers. This is possible using a pairing-based construction, first defined by Joux in 2000 [9]:

(1) Alice, Bob and Carl agree on a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)[\ell]$ of prime order such that there exists an ℓ-distortion map for P. These are the public parameters.

(2) Then Alice, Bob and Carl choose secret integers n_A, n_B, n_C and they compute $Q_A = n_A P$, $Q_B = n_B P$ and $Q_C = n_C P$, respectively. They now publish the values of Q_A, Q_B and Q_C.

(3) Alice then computes $\hat{e}_\ell(Q_B, Q_C)^{n_A}$. By the bilinearity of the modified Weil pairing we have
$$\hat{e}_\ell(Q_B, Q_C)^{n_A} = \hat{e}_\ell(n_B P, n_C P)^{n_A} = \hat{e}_\ell(P, P)^{n_A n_B n_C}.$$
Bob and Carl use their secret integers and the public points to perform similar computations.

(4) Then the three people have shared the secret value $\hat{e}_\ell(P, P)^{n_A n_B n_C}$.

If Eve can solve the ECDLP then she can break tripartite Diffie-Hellman key exchange. On the other hand Eve can use the public points Q_A and P to compute
$$\hat{e}_\ell(P, P) \quad \text{and} \quad \hat{e}_\ell(Q_A, P) = \hat{e}_\ell(n_A P, P) = \hat{e}_\ell(P, P)^{n_A}.$$
And so Eve can recover n_A if she can solve the DLP for a subgroup of $\mathbb{F}_q^*$ of order ℓ. Then the tripartite Diffie-Hellman key exchange requires q being sufficiently large. Joux's protocol can be generalized to an n-people one-round protocol by using an efficiently computable multilinear map $\hat{e}_N : G^n \longrightarrow \mu_N$. The existence of such multilinear maps for any $n > 2$ is an open question. Boneh and Silverberg [5] have given some evidence that it may not be possible to construct multilinear maps with $n > 2$ from natural maps that arise in algebraic geometry. Joux's protocol is not interesting from a practical point of view because it is only resistant to passive attacks and needs at least one additional round of communications in order to resist active attacks. Nonetheless, it serves as an elegant example of the potential of pairings in protocol design.

2.6. **ID-based Cryptography.** The goal of ID-based cryptography is to obtain a public key cryptosystem in which the user's public key can be chosen by the user itself, for example as an email address. Assume there exists a trusted authority Tom who is available to perform computations and distribute information. Tom publishes a master public key $\texttt{Tom}^{\mathrm{Pub}}$ and keeps secret an associated private key $\texttt{Tom}^{\mathrm{Pri}}$. When Bob wants to send Alice a message, he uses the master public key $\texttt{Tom}^{\mathrm{Pub}}$ and Alice's ID-based public key $\texttt{Alice}^{\mathrm{Pub}}$ (e.g. her email address) to encrypt his message. In the meantime, Alice tells Tom that she wants to use $\texttt{Alice}^{\text{Pub}}$ as her ID-based public key. Tom uses the master private key $\texttt{Tom}^{\text{Pri}}$ and Alice's ID-based public key $\texttt{Alice}^{\text{Pub}}$ to create a private key $\texttt{Alice}^{\text{Pri}}$ for Alice. Alice then uses $\texttt{Alice}^{\text{Pri}}$ to decrypt and read Bob's message.

A practical ID-based system was introduced by Boneh and Franklin in 2001. It uses pairings on elliptic curves.

(1) Tom select a finite field $\mathbb{F}_q$, an elliptic curve E, and a point $P \in E(\mathbb{F}_q)[\ell]$ of prime order such that there is an ℓ-distortion map for P. Then he publishes two hash functions H_1 and H_2 defined as follows. The first one assigns a point in $E(\mathbb{F}_q)$ to each possible user ID,

$$H_1 : \{\text{User IDs}\} \longrightarrow E(\mathbb{F}_q).$$

The second one assigns to each element of $\mathbb{F}_q^*$ a binary string of length B,

$$H_2 : \mathbb{F}_q^* \longrightarrow \{\text{bit strings of length } B\}\,.$$

(2) Tom creates his master key by choosing a secret nonzero integer s modulo ℓ and computing the point

$$P^{\text{Tom}} = sP \in E(\mathbb{F}_q).$$

Tom's master private key is the integer s and his master public key is the point P^{Tom}.

(3) Now suppose that Bob wants to send Alice a message $M \in \mathcal{M}$, where $\mathcal{M}$ is the set of all binary strings of length B, using her ID-based public key $\texttt{Alice}^{\text{Pub}}$. He computes the point

$$P^{\text{Alice}} = H_1(\texttt{Alice}^{\text{Pub}}) \in E(\mathbb{F}_q).$$

He also chooses a random nonzero number r modulo $q-1$ and computes

$$C_1 = rP \quad \text{and} \quad C_2 = M \oplus H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r),$$

where $\oplus$ is the XOR operation on bit strings. The ciphertext is the pair $C = (C_1, C_2)$.

(4) In order to decrypt Bob's message, Alice requests Tom to give her the private key $\texttt{Alice}^{\text{Pri}}$. Tom then gives her the private key as a point

$$Q^{\text{Alice}} = sP^{\text{Alice}} = sH_1(\texttt{Alice}^{\text{Pub}}) \in E(\mathbb{F}_q).$$

(5) Now Alice can decrypt Bob's message (C_1, C_2). She computes

$$\hat{e}_\ell(Q^{\text{Alice}}, C_1) = \hat{e}_\ell(sP^{\text{Alice}}, rP) = \hat{e}_\ell(P^{\text{Alice}}, P)^{rs} = \hat{e}_\ell(P^{\text{Alice}}, sP)^r = \hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r.$$

Finally she can recover the plaintext by computing

$$C_2 \oplus H_2(\hat{e}_\ell(Q^{\text{Alice}}, C_1)) = (M \oplus H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r)) \oplus H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r) = M,$$

since $M \oplus N \oplus N = M$.

While secure against eavesdroppers, this basic encryption scheme is not resistant to chosen-ciphertext attacks where the attacker, who is trying to learn some information about the plaintext that corresponds to a target ciphertext, is able to obtain the decryption of any ciphertext of its choice. For a more secure encryption scheme see [3].

2.7. **Short Signature Scheme.** A digital signature scheme allows Alice to use a private key to sign a digital document in such a way that Bob can use Alice's public key to verify the validity of the signature. A classical protocol is the following Elliptic Curve Digital Signature Algorithm (ECDSA).

(1) Alice and Bob agree on a finite field $\mathbb{F}_p$, an elliptic curve $E/\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$ of prime order N.

(2) Alice selects an integer a and computes the point $A = aP \in E(\mathbb{F}_p)$.

(3) Alice publishes the point A. This is her *public verification key.* The secret multiplier a is her *private signing key.*

(4) Alice applies a hash function to her actual document to sign in order to obtain $d \bmod N$. She chooses a random integer $k \bmod N$, she computes kP and sets

$$s_1 \equiv x(kP) \pmod N \quad \text{and} \quad s_2 \equiv (d + as_1)k^{-1} \pmod N.$$

Alice publishes the signature (s_1, s_2).

(5) Bob computes

$$v_1 \equiv ds_2^{-1} \pmod N \quad \text{and} \quad v_2 \equiv s_1 s_2^{-1} \pmod N.$$

He then computes $v_1P + v_2A \in E(\mathbb{F}_p)$ and accepts the signature as valid if $x(v_1P + v_2A) \equiv s_1 \pmod N$.

Indeed, suppose that Alice has followed the steps above. Then

$$v_1P + v_2A = ds_2^{-1}P + s_1s_2^{-1}aP = s_2^{-1}(d + as_1)P = kP.$$

Hence $x(v_1P + v_2A) = x(kP) \equiv s_1 \pmod N$.

The following result of Boneh, Lynn and Shacham [4] is an example of a short signature scheme (i.e. the signature consists of only a single point as opposed to the classic ECDSA), which gives signatures that are half the size of those produced by ECDSA.

(1) Alice and Bob agree on a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)[\ell]$ of prime order such that there exists an ℓ-distortion map for P.

(2) Alice selects an integer a and computes the point $A = aP \in E(\mathbb{F}_q)$.

(3) Alice publishes the point A. This is her *public verification key.* The secret multiplier a is her *private signing key.*

(4) Alice applies a hash function to her actual document to sign in order to obtain a point $D \in E(\mathbb{F}_q)$. She computes and publishes the signature $S = aD$.

(5) Bob accepts the signature as valid if the two quantities $\hat{e}_\ell(A, D)$ and $\hat{e}_\ell(P, S)$ are equal.

Indeed suppose that Alice has constructed A and S as in steps (2) and (4). Then

$$\hat{e}_\ell(A, D) = \hat{e}_\ell(aP, D) = \hat{e}_\ell(P, D)^a \quad \text{and} \quad \hat{e}_\ell(P, S) = \hat{e}_\ell(P, aD) = \hat{e}_\ell(P, D)^a.$$

3. Hyperelliptic Curves

Definition 13. Let X be a smooth, geometrically connected, projective curve over a field k, of genus $g \geq 1$. X is a hyperelliptic curve if there exists a finite separable morphism $X \longrightarrow \mathbb{P}^1_k$ of degree 2.

Proposition 11. *Let X be a hyperelliptic curve of genus g over a field k. Then $K(X) = k(t)[y]$ with a relation*

$$y^2 + Q(t)y = P(t) \qquad P(t), Q(t) \in k[t]$$

and $\deg Q(t) \leq g + 1, 2g + 1 \leq \deg P(t) \leq 2g + 2$.

Proof. See [[11], 7.4.24]. □

For cryptographic applications only the curves with $\deg Q(t) \leq g$ and $\deg P(t) = 2g + 1$ are considered. They have only one point at infinity.

Remark 4. As for any curve, we can attach to a hyperelliptic curve its Jacobian variety, which is an abelian variety J of dimension g such that $J(K) \cong \mathrm{Pic}^0(X_K)$ for any extension K/k verifying $X(K) \neq \emptyset$. It turns out that the map defined in Proposition 3 is in general only injective.

The group order for $J(\mathbb{F}_q)$ is approximately q^g, by a result of Weil. He proved that

$$(\sqrt{q}-1)^{2g} \leq |J(\mathbb{F}_q)| \leq (\sqrt{q}+1)^{2g}.$$

This means that it has the same size as one gets in elliptic curve cryptography working over the extension field $\mathbb{F}_{q^g}$. In other words, if g is large, one can work over a small field. On the other hand, the group operation is much more cumbersome than in the elliptic curve case and it turns out that the DLP is much easier on the jacobian of a high-genus curve than on a comparably sized group of points of an elliptic curve.

The following are the main lines of research towards achieving an efficient and secure implementation of hyperelliptic curve cryptography (HECC):

- Finding hyperelliptic curves such that the order of the group of points on the Jacobian of the curve over a finite field is divisible by a large prime. Efficient algorithms to count points on the Jacobian of hyperelliptic curves of higher genus were proposed by Schoof, Elkies and Atkin, Gaudry and Harley, Kedlaya, Weng, Denef-Vercauteren.

- Security of HECC and its comparison with the security of ECC. The work of Gaudry, Hess and Smart have shown that Jacobians of hyperelliptic curves of genus higher than 4 are amenable to attack. This attack, known as Weil-Descent (or GHS) attack, has better complexity than the general attacks. Furthermore, Thériault has shown that, in order to achieve cryptographic security equivalent to the one provided by an elliptic curve defined over a field of size $\log q$ it is necessary to use a hyperelliptic curve of genus 3 defined over a field of size at least $\frac{7\log q}{20}$.

- Algorithms for the arithmetic on the Jacobian. There is a generic algorithm by Cantor for the arithmetic on Jacobians of curves of any genus. Subsequently it was improved by several other people.

The three protocols presented in the section above make critical use of supersingular elliptic curves and Weil pairings. It was an open question whether or not these schemes could be improved (more security for the same signature size or efficiency) using abelian varieties in place of elliptic curves. Rubin and Silverberg gave an affirmative answer in [13]. Weil pairings exist and have similar properties for abelian varieties that they have for elliptic curves. Potentially, abelian varieties can be utilized in all the applications described above to give better results (e.g., shorter signatures, or shorter ciphertexts) for the same security.

References

1. A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique I*, Springer-Verlag, 1971.
2. A. Balog, A. Cojocaru and C. David, *Average Twin Prime Conjecture for Elliptic Curves*, to appear, American Journal of Mathematics.
3. D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology - CRYPTO 2001, Lecture Notes in Computer Science, 2139 (2001), 213-229.
4. D. Boneh, B. Lynn and H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, 2248 (2001), 514-532.
5. D. Boneh and A. Silverberg, *Applications of Multilinear Forms to Cryptography*, Contemporary Mathematics, 324 (2003), 71-90.
6. A. C. Cojocaru, *Reductions of an Elliptic Curve With Almost Prime Orders*, Acta Arithmetica, 119 (2005), 265-289.
7. R. Hartshorne, *Algebraic Geometry*, Springer, 1977.
8. J. Hoffstein, J. Pipher and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008.
9. A. Joux, *A One Round Protocol for Tripartite Diffie-Hellman*, Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, 1838 (2000), 385-393.
10. N. Koblitz, A. Menezes and S. Vanstone, *The State of Elliptic Curve Cryptography*, Designs, Codes and Cryptography, 19 (2000), 173-193.
11. Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2006.

12. A. Menezes, T. Okamoto and S. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Transactions on Information Theory, 39 (1993), 1639-1646.
13. K. Rubin, A. Silverberg, *Using Abelian Varieties to Improve Pairing-based Cryptography*, Journal of Cryptology, 22 (2009), 330-364.
14. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009.
15. J. Scholten and F. Vercauteren, *An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem*, available at http://homes.esat.kuleuven.be/ fvercaut/papers/cc03.pdf.
16. R. Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Math. Comp., 44 (1985), 483-494.
17. V. Shoup, *Lower Bounds for Discrete Logarithms and Related Problems*, Advances in Cryptology - EUROCRYPT 1997, Lecture Notes in Computer Science, 1233 (1997), 256-266.
18. J. H. Silverman and J. Suzuki, *Elliptic Curve Discrete Logarithms and the Index Calculus*, Advances in Cryptology - ASIACRYPT 1998, Lecture Notes in Computer Science, 1514 (1998), 110-125.
19. E. R. Verheul, *Evidence that XTR is More Secure than Supersingular Elliptic Curve Cryptosystem*, Journal of Cryptology, 17 (2004), 277-296.