1 Algebraic constructions

An apt quote "the Weil pairing is just two applications of the Tate pairing" describes clearly the connection between Weil and Tate pairings. First we define some useful algebraic constructions and then we can define the Weil and the Tate pairing.

1.1 Elliptic curves

The elliptic curve is a projective variety that is defined by the *Weierstrass* equation

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x_2 + a_4x + a_6, \qquad a_i \in \mathbb{F}_q. \tag{1}$$

More precisely we are interested in *non-singular elliptic curves*, that is the curve must have no points, where all partial derivatives of the corresponding homogeneous equation will vanish (The non-singularity has a straightforward criteria). The curve E has one infinity point $\mathcal{O}$ and all other points $P = (x, y)$ that satisfy the equation (1), where x and y is taken from the algebraic closure $\overline{K}$ of $\mathbb{F}_q$. Many points in the elliptic curve have coordinates from extensions of $\mathbb{F}_q$. Therefore we denote by $E(\mathbb{F}_q)$ all $\mathbb{F}_q$-rational points, that is

$$E(\mathbb{F}_q) = \{(x, y) \in E \mid x, y \in \mathbb{F}_q\} \cup \{\mathcal{O}\}.$$

In a similar manner, we define L-rational points

$$E(L) = \{(x, y) \in E \mid x, y \in L\} \cup \{\mathcal{O}\},$$

where $\mathbb{F}_q \subseteq L$ is a field extension of the field $\mathbb{F}_q$. Hasse's theorem gives a good bound to the number of $\mathbb{F}_q$-rational points. The elliptic curve is said to be *supersingular* if $\#E(\mathbb{F}_q) \equiv 1 \mod p$, where p is the characteristic of $\mathbb{F}_q$.

Points of the elliptic curve form a group, where addition is defined by the specific rule. The formal law ensures that rational points $E(L)$ are sub-groups of E and that the zero element is the infinity point $\mathcal{O}$. Now consider a *r-torsion sub-group*

$$E[r] = \{P \in E \mid rP = \mathcal{O}\}$$

If r and q are coprime numbers then the $E[r] \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$ and $E[r]$ is finite. Therefore exist a finite field extension $\mathbb{F}_{q^k}$ so that $E[r] \subseteq E(\mathbb{F}_{q^k})$.

1.2 Properties of r-torsion subgroup

Let r be a prime number then for an arbitrary extension L the intersection of $E(L)[r] = E[r] \cap E(L)$ can be isomorphic to 0, $\mathbb{Z}_r$ or $\mathbb{Z}_r \oplus \mathbb{Z}_r$. For the Tate pairing we need $\#E(L) = r$. There are two possible ways to achieve the goal: first one can search a subgroup of $E(\mathbb{F}_q)$ with the order r or otherwise take the whole group $E(\mathbb{F}_q)$. The construction of Tate pairing favors supersingular curves defined in Table 1.

Curve	Field	Order	k
$y^2 = x^3 + x$	$\mathbb{F}_p$	$p + 1$	2
$y^2 + y = x^3 + x$	$\mathbb{F}_{2^m}$	$2^m + 1 + 2^{(m+1)/2}$	4
$y^2 + y = x^3 + x + 1$	$\mathbb{F}_{2^m}$	$2^m + 1 - 2^{(m+1)/2}$	4
$y^2 = x^3 - x + 1$	$\mathbb{F}_{3^m}$	$3^m + 1 + 3^{(m+1)/2}$	6
$y^2 = x^3 - x - 1$	$\mathbb{F}_{3^m}$	$3^m + 1 - 3^{(m+1)/2}$	6

Figure 1: Suitable supersigular curves for Tate pairing

Let k be the smallest exponent so that all rth roots of unity are in $\mathbb{F}_{q^k}$. Then $E(\mathbb{F}_{q^s})$ where $s < k$ cannot contain the entire r-torsion group $E[r]$. The proof is follows from the construction of the Wail pairing. If the $E[r] \subseteq E(\mathbb{F}_{q^s})$ then we can construct Weil paring $e_r : E[r] \times E[r] \to \mathbb{F}_{q^s}$ and there exist points $S, T \in E[r]$ such that $e_r(S, T)$ is a primitive rth root of unity [Sil86, p. 98]. Consequently $r \mid q^s - 1$ what impossible. For the curves in Table 1 the $E(\mathbb{F}_{q^k})$ contains entire r-torsion group, since there is a nontrival authomorphis ϕ maps $E(\mathbb{F}_q)$ to a different subgroup.

1.3 Function field and divisors

The function field and divisors are final algebraic ingredients of the Tate pairing. Let $\overline{K}$ be the algebraic closure of $\mathbb{F}_q$. Then the polynomials that are constantly zero on the elliptic curve E form an ideal I of $\overline{K}[x, y]$, where

$$I = I\big(E/\overline{K}\big) = \big\{f \in \overline{K}[x, y] \mid \forall P \in E : \ f(P) = 0\big\}\,.$$

The ideal I allows to define integral domain $\overline{K}[E] = \overline{K}[X]/I$, since there is no zero divisors(The fact itself is nontrivial). Hence the quotiont field

$$\overline{K}(E) = \left\{ \frac{f_1(x,y)}{f_2(x,y)} + I \middle| f_1, f_2 \in \overline{K}[x,y],\ f_2 \notin I \right\}$$

exists. The *function field* of the elliptic curve is $K(E)$. Note that for every curve point $P \in E$ the value $[f+I](P)$ is well defined, since for all polynomials $g \in I$ the value $g(P) = 0$.

The *order* $\mathrm{ord}_p(f)$ of a polynomial $f \in \overline{K}[E]$ at point $P \in E$ is defined formally as a maximum number $d \in \mathbb{N}_0$ so that

$$f + I \in M_P^d, \qquad \text{where} \quad M_p = \left\{ g + I \in \overline{K}[X]/I : [g+I](P) = 0 \right\}.$$

Intuitively it captures how many "zero points of f" are in P. For rational function $f_1/f_2 + I$ the order is extended

$$\mathrm{ord}_P\big(f_1/f_2 + I\big) = \mathrm{ord}_P(f_1 + I) - \mathrm{ord}_P(f_2 + I).$$

Divisors are just formal sums of curve points. More pecisely, the divisor group of curve E is

$$\mathrm{Div}(E) = \left\{ D = \sum_{P \in E} n_P(P) \;\middle|\; \text{Number of nonzero terms is finite} \right\}.$$

The *degree* of divisor is just the sum of all coefficients

$$\deg D = \sum_{P \in E} n_P$$

which is finite. Clearly, all divisors with degree 0 form a subgroup $\mathrm{Div}^0(E)$.

Every rational function in the function field $\overline{K}(E)$ has a corresponding *divisor*

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$$

Divisor $D \in \mathrm{Div}^0(E)$ is called a *principal divisor* if exists rational function $f \in \overline{K}(E)$ such that $D = \mathrm{div}(f)$.Two divisors D_1 and D_2 are called *linearly equivalent* if $D_1 - D_2$ is a principal divisor. The linear equivalence is denoted by $D_1 \sim D_2$. Principal divisors form a subgroup of $\mathrm{Div}(E)$, since the equation $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$ holds. The divisor$D$ is principal divisor if $\deg D = 0$ and nonformal sum of the divisor is $\mathcal{O}$.

The *support* of the divisor is the set of the curve points that have nonzero coefficients. The *support* of the function f is just the support of $\operatorname{div}(f)$. If supports the divisor D and function f are disjoint we can define *evaluation*

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

2 Definition of Tate pairing

Definition 1. Let $G = E(L)$ such that $E[r] \subseteq G$. The Tate pairing is a function $\widehat{e} : G[r] \times G/rG \to \mathbb{F}_{q^k}^*$ defined as follows. Given a point $P \in G[r]$, there exists function $f \in \mathbb{F}_{q^k}(E)$ such that $\operatorname{div}(g) = r(P) - r(\mathcal{O})$. Let D be such a divisor that $D \sim (Q) - (\mathcal{O})$ and that the support of D is disjoint from the support of f. Then the value of Tate pairing is $\widehat{e}(P, Q) = f(D)^{(q^k-1)/l}$.

As the supports are different the evaluation $f(D)$ exists. We do not proove but it is possible to find D which support is in $E(\mathbb{F}_{q^k})$. The existance of the function $f \in \mathbb{F}_{q^k}(E)$ follows from the Miller's algorithm. Since $f \in \mathbb{F}_{q^k}(E)$ and $D \in \mathbb{F}_{q^k}$ the value $f(D) \in \mathbb{F}_{q^k}^*$. Secondly, the value does not depend on the function f as long as $\operatorname{div}(f) = r(P) - r(\mathcal{O})$. Let two functions f_1 and f_2 have the same divisor. Then it follows $f_1 = \alpha f_2$, where $\alpha \in \mathbb{F}_{q^k}$. Now since D has a zero degree

$$f_1(D) = \prod_{\substack{P \in E \\ n_P \neq 0}} \alpha^{n_p} f_2(P)^{n_p} = \prod_{\substack{P \in E \\ n_P \neq 0}} f_2(P)^{n_p} = f_2(D).$$

We dont proove that the $\widehat{e}(P, Q)$ does not depend on the divisior D. But the independece of $\widehat{e}(P, Q)$ is equivalent to the following condition. For every principal divisor D_1 which support is in $E(\mathbb{F}_{q^k})$ and is disjoint from $r(P) - r(\mathcal{O})$ the evaluation $f(D_1)$ is rth root of unity. The claim follows from the lineary of the evaluation map

$$f(D)^{(q^k-1)/l} f(D_1)^{(q^k-1)/l} = f(D + D_1)^{(q^k-1)/r} = \widehat{e}(P, Q) = f(D)^{(q^k-1)/r}.$$

2.1 Properties

Well defined For all $P \in G[r]$ and $Q \in G$ the equations $\widehat{e}(\mathcal{O}, Q) = 1$ and $\widehat{e}(P, rQ) = 1$ hold. The first property is evident since f must be a constant function. 0. The latter equation follows from the decomposition

$$D_2 = (rQ) - \mathcal{O} = \underbrace{r(Q) - r(\mathcal{O})}_{\sim rD} + \underbrace{(rQ) - r(Q) + (r-1)(\mathcal{O})}_{D_1},$$

since D_1 is principal divisor with disjoint support we get

$$f(D_2)^{(q^k-1)/r} = f(rD)^{(q^k-1)/r} f(D_1)^{(q^k-1)/r} = 1.$$

If supports of D_1 and f are not disjoint then there are only two altenatives $rQ = P$ or $Q = P$. For the first alternative we choose the divisor differently

$$\begin{aligned} D_2 &\sim (r^2Q) - (r(r-1)Q) = (\mathcal{O}) - ((r-1)rQ) \\ &= \underbrace{-r((r-1)Q) + r(\mathcal{O})}_{\sim rD'} + \underbrace{r((r-1)Q) - (r(r-1)Q) - (r-1)\mathcal{O}}_{D_1'}. \end{aligned}$$

Now the supports of D_1' and f are disjoint unless $P = \mathcal{O}$. The latter condition forces $rQ = \mathcal{O}$ that implies $D_2 = 0$.

Non-degerancy:. For each point $P \in G[l] \setminus \mathcal{O}$ there exists $Q \in G$ such that $\widehat{e}(P, Q) \neq 1$. The corresponding non-elementary proof can be found [tat].

Bilinearity: For any integer n

$$\widehat{e}(nP, Q) = \widehat{e}(P, Q)^n = \widehat{e}(P, nQ).$$

Let $[n]$ be a rational function $[n](x, y) = (nx, ny)$ and $\mathrm{div}(f) = r(P) - r(\mathcal{O})$. Then $f \circ [n]$ has divisor $r(nP) - r(\mathcal{O})$ and consequently

$$\widehat{e}(nP, Q) = f([n]D)^{(q^k-1)/l} = f(D)^{n(q^k-1)/l},$$

since $[n]D - nD$ is principal divisor and $[n]D = nD + ([n]D - nD)$. The second equation follows since the divisor $[n]D$ corresponds to nQ. Again divisors with intersecting supports must be treated differently. Notice that the bilinarity does not guarantee $\widehat{e}(P, S + T) = \widehat{e}(P, S)\widehat{e}(P, T)$ unless S and T are taken from the cyclic group. Hence cryptographic applications use only restriction of the Tate pairing.

3 Square-and-multiply algoritm

3.1 Divisors of stright lines

Miller's algorithm uses divisors of stright lines. The number of intersection points of elliptic curve and stright line is always three. The line $l_{P,Q}$, that goes through points P and Q of the curve E, has third intersection point at $(-P-Q)$. If $P = Q$ then the line $l_{P,P}$ is taken as tangent to the curve E and the third intersection point $-2P$. Of course, the lines can be represented as first degree polunomials that belong to the function field.

The divisor of the line can be calculated by the following rule. The divisor of a stright line l that intersects with elliptic curve in theree points P_1, P_2 and P_3 has following form

$$\mathrm{div}(l_{P_1,P_2}) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}).$$

The formula is correct even if $P_1 = P_2$ or $P_i = \mathcal{O}$ but formal addition gives a bit different form

$$\begin{aligned}\mathrm{div}(l_{P,P}) &= 2(P) + (-2P) - 3\mathcal{O},\\ \mathrm{div}(l_{P,\mathcal{O}}) &= (P) + (-P) - 2\mathcal{O}.\end{aligned}$$

The informal justification is simple. In each intersection point $l_{P,Q}$ has a zero and is well-defined in other points except in the infinity point, where it must have poles. Since $\deg(\mathrm{div}(l)) = 0$ the number of poles must be equal to number of zeroes. If line is tangent to E at point P then there is a double zero at point P.

3.2 Miller's algorithm

The original Miller's algorithm is very similar to fast exponentiation algorithm. Recall that we must calculate $f(D)$, where $\mathrm{div}(f) = l(P) - l(\mathcal{O})$, and D is linearly equvalent to the divisor $(Q) - (\mathcal{O})$. For a random point $S \in E(\mathbb{F}_{q^k})$ and $Q' = S + Q$ the divisors $D_1 = (Q') - (S)$ and $D = (Q) - (\mathcal{O})$ linearly equivalent, since the non-formal sum $D_1 - D = Q' - S - Q + \mathcal{O} = \mathcal{O}$. Therefore we can calculate $e(P, Q) = f(D_1)$ as long the supports of g and D_1 are different.

We decribe the algorithm that evaluates $f(R)$ for an arbitrary $R \in G$, since $f(D)$ is a product of $f(R)^{n_R}$. The Miller's algorithm evaluates $f(R)$ using square-and-multiple technique. The function f is iteratively constructed from first degree polynomials that correspond to straight lines. In principle, the algoritm can fail if intermediate support of f contains R. Then either divison by zero happens or the end result is zero. But both failures are easily detectable. Secondly, as the S was chosen randomly the collision probablity is small.

Algorithm 1: Square-and-multiple algorithm

Input: The r-torsion point $P \in G[r]$ and $R \in G$
Output: The value $f(R)$, where $\operatorname{div}(f) = r(P) - r(\mathcal{O})$.

$n \leftarrow \lfloor \log r \rfloor$
$V \leftarrow P$; $f \leftarrow 1$
▲▲▲ Let $\overline{r_0 \dots r_n}$ be the binary repr. of r ▲▲▲
for $i = 1$ ***to*** n **do**
  $f \leftarrow f^2 \cdot l_{V,V}(R)/l_{2V,\mathcal{O}}(R)$
  $V \leftarrow 2V$
  if $r_i = 1$ **then**
    $f \leftarrow f \cdot l_{V,P}(x,y)/l_{V+P,\mathcal{O}}(R)$
    $V \leftarrow V + P$
return f

3.3 Correctness

We show that the algorithm calculates the correct value. Let $\overline{r_0 \dots r_n}$ be the binary representation of r and $a_i = \overline{r_0 \dots r_i}$. Let f_i be the function corresponding to f at the end of the ith cycle. First the lines implement addition and

$$\operatorname{div}(l_{V,V}/l_{2V,\mathcal{O}}) = 2(V) - (2V) - \mathcal{O}$$
$$\operatorname{div}(l_{V,P}/l_{V+P,\mathcal{O}}) = (V) + (P) - (V+P) - \mathcal{O}.$$

If the bit $l_i = 0$ then

$$\operatorname{div}(f_i) = \operatorname{div}(f_{i-1}^2 \cdot l_{V,V}/l_{2V,\mathcal{O}}) = 2\operatorname{div}(f_{i-1}) + 2(a_{i-1}P) - (a_iP) - \mathcal{O},$$

otherwise

$$\begin{aligned}\operatorname{div}(f_i) &= \operatorname{div}(f_{i-1}^2 \cdot l_{V,V}/l_{2V,\mathcal{O}} \cdot l_{2V,P}/l_{2V+P,\mathcal{O}}) \\ &= 2\operatorname{div}(f_{i-1}) + 2(a_{i-1}P) - (2a_{i-1}P) - \mathcal{O} + (2a_{i-1}P) + (P) - (a_iP) - \mathcal{O} \\ &= 2\operatorname{div}(f_{i-1}) + 2(a_{i-1}P) + (P) - (a_iP) - 2\mathcal{O}.\end{aligned}$$

Simple induction gives $\operatorname{div}(f_i) = a_i(P) - (a_iP) - (a_i - 1)(\mathcal{O})$. Therefore the returned function $f = f_n$ satisfies $\operatorname{div}(f) = l(P) - l(\mathcal{O})$, since $lP = \mathcal{O}$. The correctness is proved.

Notice that if $R \notin \langle P \rangle$ and $R \neq \mathcal{O}$ the calcucation never fails. The **complexity** is $\mathcal{O}(\log r)$ operations in the field $\mathbb{F}_{q^k}$. $\square$

4 Cube-and-multiply algorithm

The supersingular curves $E : y^2 = x^3 - x \pm 1$ over $\mathbb{F}_{3^m}$ favor the tripling, since calculation of $3P$ can be done extreamly fast. There exists tripling formula which does not contain divisions! Namely, if $P = (x, y)$ then $3P = (x_3, y_3)$, where $x_3 = x_1 + y_1^2 + y_1^6$ and $y_3 = -y_1^9$. Notice that cubing can be done in the linear time, since the caracteristic is 3. Also the stright lines $l_{V,V}$ and $l_{V,2V}$ can be calculated with only one division. Therefore generalised Miller's algorithm was developed [GHS02].

Let $l = \overline{r_0 \dots r_n}$ be the trinary representation of r, where $r_i \in \{-1, 0, 1\}$ and $r_0 = 1$. Hence $n = \lfloor \log_3 r \rfloor$.

Algorithm 2: Cube-and-multiply algorithm

Input: The r-torsion point $P \in G[r]$ and $R \in G$
Output: The value $f(R)$, where $\mathrm{div}(f) = r(P) - r(\mathcal{O})$.

$n \leftarrow \lfloor \log_3 r \rfloor$
$V \leftarrow P$; $f \leftarrow 1$
▲▲▲ The divisor $\mathrm{div}(g) = -(P) - (-P) + 2\mathcal{O}$ ▲▲▲
$g \leftarrow 1/(x - x_P)$
▲▲▲ Let $r = \overline{r_0 r_1 \dots r_n}$ be the trinary repr., ▲▲▲
▲▲▲ where $r_i \in \{-1, 0, 1\}$ and $r_0 = 1$ ▲▲▲
for $i = 1$ ***to*** n **do**
  $f \leftarrow f^3 \cdot l_{V,V}/l_{2V,\mathcal{O}} \cdot l_{V,2V}/l_{3V,\mathcal{O}}(R)$
  $V \leftarrow 3V$
  if $r_i = 1$ **then**
    $f \leftarrow fg \cdot l_{V,P}/l_{V+P,\mathcal{O}}(R)$
    $V \leftarrow V + P$
  else if $r_i = -1$ **then**
    $f \leftarrow fg \cdot l_{V,-P}/l_{V-P,\mathcal{O}}(R)$
    $V \leftarrow V - P$
return f

4.1 Correctness

Let a_i be the truncated number $a_i = \overline{r_0 \dots l_i}$ and f_i the function corresponding to f at the end of the ith cycle. Simple calculation shows that

$$\begin{aligned}
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) - (a_iP) - 2\mathcal{O}, && r_i = 0,\\
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) + (P) - (a_iP) - 3\mathcal{O}, && r_i = 1,\\
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) - (P) - (a_iP) - 3\mathcal{O}, && r_i = -1.
\end{aligned}$$

Note that the last equation holds, since f is multiplied with g. Staightforward induction gives $\operatorname{div}(f_i) = a_i(P) - (a_iP) - (a_i - 1)(\mathcal{O})$. Therefore the returned function $f = f_n$ satisfies $\operatorname{div}(f) = l(P) - l(\mathcal{O})$. Again if $R \notin \langle P \rangle$ the calculation never fails. The **complexity** is $\mathcal{O}(\log_3 l)$ operations in the field $\mathbb{F}_{q^k}$. $\square$

5 Optimization techniques

In the Miller's algorithm we have to distinct values $V \in G[r]$ and $f \in E(\mathbb{F}_{q^k})$. If $P \in E(\mathbb{F}_q)$ then the value V remains into $E(\mathbb{F}_q)$ and we can calculate multiples of V using operations of $\mathbb{F}_q$. Further if E is a supersingular curve and $k > 1$ then half of the calculation can be skipped. Shortly put $\widehat{e}(P, Q) = f(Q)^{(q^k-1)/l}$. Recall that $k \in \mathbb{N}_0$ is a minimum number so that $r \mid q^k - 1$ but $r \not| q^s - 1$, where $s < k$.

First it is possible to choose r such that $q - 1 \mid (q^k - 1)/r$ and then the following theorem holds, see [BKLS] for further details.

Theorem 1. *Let P be from an r-element sub-group $G_1 \subseteq E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. Then $\widehat{e}(P, Q) = f(Q)^{(q^k-1)/l}$, where* $\operatorname{div}(f) = l(P) - l(Q)$.

Another optimization is to take r element sub-group $G_2 \subseteq E(\mathbb{F}_{q^k})$ so that $G_2 = \phi(G_1)$. Also as $G_1 \cap G_2 =$ the intermidiate divisors in the Miller's algorithm do not contain Q and failure can never happen. For supersingular elliptic curves from Table 1 special authomorphism are constructed so that $\phi(G_1) \not\subseteq rG$, see article [BKLS] for future references.

Theorem 2. *Let the elliptic curve be one from the table and ϕ the corresponding authomorphism of $E(\mathbb{F}_{q^k})$. If $P \in G_1$ and $Q \in phi(G_1)$ then the denominators $l_{V,\mathcal{O}}(\psi(Q))$ and $l_{V+P,\mathcal{O}}(\psi(Q))$ and can be discarded in the Miller's algorithms.*

The proof bases on the fact that the order of denominators divides $(q^k - 1)/r$ and therefore the contribution to the Tate pairing is 1. The proof uses properties of ϕ and the fact that the denominators correspond to vertical lines. Therefore in the optimized Miller's algorithm are no divisions! This is remarcable improvent since the division takes more time than multiplication. Also the formulas for the authomorphism are simple. For example the first curve from Table 1 uses the $\phi = (-x, iy)$, where $i \in \mathbb{F}_p$ and $i^2 = 1$.

Primes with low weight: The basic Miller's algorithm does an additional multiplication if $r_i = 1$. Therefore it is natural to seek primes r with low Hamming weight. The supersingular curves from Table 1 have this property, since group orders $2^m \pm 2^{(m+1)/2+1}$ and $3^m \pm 3^{(m+1)/2} + 1$ have very low Hamming weight. The number of multiplications drops signifficantly. Moreover, in the article [DL03] closed formula of the Tate pairing for supersingular curve $y^2 = x^3 - x \pm 1$ over $\mathbb{F}_{3^m}$ is obtained.

References

[BKLS] Paulo S.L.M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems.

[DL03] Iwan Duursma and Hyang-Sook Lee. Tate-pairing implementations for tripartite key agreement. Cryptology ePrint Archive, Report 2003/053, 2003. `http://eprint.iacr.org/`.

[GHS02] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the tate pairing. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 2002.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[tat]