Tate-pairing implementations for tripartite key agreement

Iwan Duursma
Dept. of Mathematics, University of Illinois at Urbana Champaign
IL. 61801, USA
Hyang-Sook Lee
Dept. of Mathematics, Ewha Womans University
Seoul, 120-750, Korea

Abstract – We give a closed formula for the Tate-pairing on the hyperelliptic curve $y^2 = x^p - x + d$ in characteristic p. This improves recent implementations by Barreto et.al. and by Galbraith et.al. for the special case $p = 3$. As an application, we propose a n-round key agreement protocol for up to 3^n participants by extending Joux's pairing-based protocol to n rounds.

Keywords – elliptic curve cryptosystem, Tate pairing implementation, bilinear Diffie-Hellman problem, group key agreement protocol

1 Introduction

Pairings were first used in cryptography as a cryptanalytic tool for reducing the discrete log problem on some elliptic curves to the discrete log problem in a finite field. There are two reduction types. One uses the Weil pairing and is called the MOV reduction [MOV93], the other uses the Tate pairing and is called the FR reduction [FR94]. Positive cryptographic applications based on pairings followed from the work of Joux [J00], who gave a simple one-round tripartite Diffie-Hellman protocol on supersingular curves.

Curve-based pairings, such as the Weil-pairing and Tate-pairing, provide a good setting for the so-called bilinear Diffie-Hellman problem. Important cryptographic protocols using pairings include ID based encryption [BF01], signature schemes [SOK00], [H02a], [P02], [CC03] and key exchange [S02]. For the practical applications of those systems it is important to have efficient implementations of the pairings. According to [G01], the Tate pairing can be computed more efficiently than the Weil pairing. The recent papers [BKLS02], [GHS02] provide fast computations of the Tate pairing in characteristic three.

Our main result in this paper is an expression for the Tate-pairing on the hyperelliptic curve defined by the equation $C^d/k : y^2 = x^p - x + d$, for a prime number p congruent to 3 modulo 4 (Theorem 4). We assume that k is a finite extension of degree n of the prime field F_p with n coprime to $2p$. The formula assigns to a pair (P, Q) of k-rational points on the curve an element $\{P, Q\} \in K^*$, where K/k is an extension of degree $2p$. By a general property of the Tate-pairing the map is bilinear. Following Joux [J00], we can use the map to define a tripartite key agreement protocol: If A, B, C are three parties with private keys a, b, c, and public keys aP, bP, cP, respectively, they can establish a common secret key $\alpha \in K^*$ via

$$\alpha = \{aP, bP\}^c = \{bP, cP\}^a = \{cP, aP\}^b \in K^*.$$

The computation of the Tate pairing can be performed using an algorithm first presented by Miller [M86]. For a general elliptic curve in characteristic three, the computation can be improved. For the elliptic curve $E^b/k : y^2 = x^3 - x + b$, techniques specific to the curve yield further improvements [BKLS02], [GHS02]. We describe these algorithms and we show that the evaluation of our expression, for the special case $p = 3$, uses fewer logical and arithmetic operations. Our main motivation to study pairings is for multi-party key agreement protocols. Thus we present a protocol whereby a group of at most 3^n users can agree on a common secret in no more than n rounds. The main idea is to use the pairing-based one-round tripartite Diffie-Hellman protocol [J00] multiple times.

In the next section, we recall the general formulation of the Tate-pairing and Miller's algorithm in base 2 (Algorithm 1). Section 3 gives useful properties of the elliptic curve $E^b : y^2 = x^p - x + b$ and gives Miller's algorithm in base 3 (Algorithm 2). Section 4 describes the algorithm for computing the Tate-pairing proposed by Barreto et al. [BKLS02] (Algorithm 3). Section 5 gives useful properties of the curve $C^d : y^2 = x^p - x + d$ and we give a first algorithm to evaluate the Tate-pairing for the curve C^d (Algorithm 4). Our main result in Section 6 gives the output of this algorithm in closed form. The expression is then used to formulate Algorithm 5, which is faster than the previous algorithms. For comparison, we derive in Appendix A a closed expression for the output of the algorithm proposed by Barreto et al. Section 7 describes the application of curve-based pairings to bilinear Diffie-Hellman problems. In Section 8 we present a n-round key-agreement protocol for up to 3^n users.

2 Tate-pairing

Let X/k be an algebraic curve over the finite field k. Let **Div** be the group of divisors on X, $\mathbf{Div_0}$ the subgroup of divisors of degree zero, **Prin** the subgroup of principal divisors, and $\Gamma = \mathbf{Div_0}/\mathbf{Prin}$ the group of divisor classes of degree zero. For $m > 0$ prime to char k, let

$$\Gamma[m] = \{[D] \in \Gamma : mD \text{ is principal}\}.$$

For a rational function f and a divisor $E = \sum n_P P$ with $(f) \cap E = \emptyset$, let

$$f(E) = \prod f(P)^{n_P} \in k^*.$$

Theorem 1 ([FR94], [H02b]) *The Tate-pairing*

$$\begin{aligned} \{-,-\}_m : \quad & \Gamma[m] \times \Gamma/m\Gamma \longrightarrow k^*/k^{*m}, \\ & \{[D],[E]\}_m = f_D(E), \end{aligned}$$

is well-defined on divisor classes. The pairing is non-degenerate if and only if the constant field k of X contains the m-th roots of unity. Here, f_D is such that $(f_D) = mD$, and we assume that the classes are represented by divisors with disjoint support: $D \cap E = \emptyset$.

For an elliptic curve E/k we can identify Γ with the group of rational points on the curve using an isomorphism $E(k) \simeq \Gamma$, $P \mapsto [P - O]$. For an elliptic curve E/k, and for $D = [P - O]$, efficient computation of $f_D(Q)$ in the Tate-pairing is achieved with a square-and-multiply strategy using Miller's algorithm (Algorithm 1).

3 The elliptic curve $E : y^2 = x^3 - x + b$

Let $E^+ : y^2 = x^3 - x + 1$ and $E^- : y^2 = x^3 - x - 1$ be twisted elliptic curves over the field F_3 of three elements. Their cryptographic applications have been studied in [K98], [DS98]. For the number of points on E^+ or E^- over an extension field $k = F_{3^n}$ such that $(n, 6) = 1$ we have

$$|E^+(F_{3^n})| = \begin{cases} 3^n + 1 + 3^{(n+1)/2} & \text{if } n \equiv 1, 11 \pmod{12}, \\ 3^n + 1 - 3^{(n+1)/2} & \text{if } n \equiv 5, 7 \pmod{12}. \end{cases}$$

$$|E^-(F_{3^n})| = \begin{cases} 3^n + 1 - 3^{(n+1)/2} & \text{if } n \equiv 1, 11 \pmod{12}, \\ 3^n + 1 + 3^{(n+1)/2} & \text{if } n \equiv 5, 7 \pmod{12}. \end{cases}$$

In each case, the group order N divides $3^{3n} + 1$, as can be seen from the following identity, applied with $T = 3^{(n-1)/2}$,

$$(1 + 3^3 T^6) = (1 + 3T^2)(1 + 3T + 3T^2)(1 - 3T + 3T^2).$$

Thus the Tate-pairing

$$\begin{aligned} \{-,-\}_N : \quad & \Gamma[N] \times \Gamma/N\Gamma \longrightarrow K^*/{K^*}^N, \\ & \{[D],[E]\}_m = f_D(E), \end{aligned}$$

is non-degenerate for an extension K/k of degree $[K : k] = 6$. For the extension K/k, $E(K)$ contains the full N-torsion and the Weil-pairing is also non-degenerate [MOV93].

For the curves E^b, $b = \pm 1$, multiplication $V \mapsto 3V$ is particularly simple. For $V = (\alpha, \beta)$, $3V = (\alpha^9 - b, -\beta^9)$. Also, taking the cube of a scalar $f \mapsto f^3$ in characteristic three has linear complexity on a normal basis. Thus, Miller's algorithm will perform faster for these curves in a cube-and-multiply version (Algorithm 2).

4 The BKLS-Algorithm

We will describe further improvements to Algorithm 2 proposed in [BKLS02], [GHS02]. In this section, we deal with the curve $E^b/k : y^2 = x^3 - x + b$, for $b = \pm 1$. We assume k is of finite degree $[k : F_3] = n$ with $\gcd(n, 6) = 1$. And we let F/k and K/k be extensions of degree $[F : k] = 3$ and $[K : k] = 6$, respectively. The following theorem and lemma are similar to Theorem 1 and Lemma 1, respectively, in [BKLS02].

Algorithm 1 Miller's algorithm, square-and-multiply [M86]

INPUT: $P, Q \in E(K), (a_i) \in \{0,1\}^s$.

$\{a = 2^s + a_1 2^{s-1} + \cdots + a_{s-1}2 + a_s.\}$

OUTPUT: $f_a(Q)$.

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (l_{A,B}) = A + B + (-A-B) - 3O.\}$

$a \leftarrow 1,\ V \leftarrow P,\ f \leftarrow 1$
for $i = 1$ to s **do**
  $g \leftarrow l_{V,V}/l_{2V,O}(Q)$
  $a \leftarrow 2a,\ V \leftarrow 2V,\ f \leftarrow f^2 \cdot g$
  if $a_i = 1$ **then**
    $g \leftarrow l_{P,V}/l_{V+P,O}(Q)$
    $a \leftarrow a+1,\ V \leftarrow V+P,\ f \leftarrow f \cdot g$
  end if
  $\{a \leftarrow 2^i + a_1 2^{i-1} + \cdots + a_{i-1}2 + a_i,\ V \leftarrow aP,\ f \leftarrow f_a(Q).\}$
end for

Algorithm 2 Miller's algorithm, cube-and-multiply [GHS02], [BKLS02]

INPUT: $P, Q \in E(K), (a_i) \in \{0,\pm 1\}^s$.

$\{a = 3^s + a_1 3^{s-1} + \cdots + a_{s-1}3 + a_s.\}$

OUTPUT: $f_a(Q)$.

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (l_{A,B}) = A + B + (-A-B) - 3O.\}$

$a \leftarrow 1,\ V \leftarrow P,\ f \leftarrow 1$
for $i = 1$ to s **do**
  $g \leftarrow l_{V,V}/l_{2V,O} \cdot l_{V,2V}/l_{3V,O}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g$
  if $a_i = \pm 1$ **then**
    $g \leftarrow l_{\pm P,V}/l_{V\pm P,O}(Q)$
    $a \leftarrow a \pm 1,\ V \leftarrow V \pm P,\ f \leftarrow f \cdot g$
  end if
  $\{a \leftarrow 3^i + a_1 3^{i-1} + \cdots + a_{i-1}3 + a_i,\ V \leftarrow aP,\ f \leftarrow f_a(Q).\}$
end for

Theorem 2 *Let $N = |E(k)|$. Let $P, O \in E(k)$ be distinct points, and let g_P be a k-rational function with $(g_P) = N(P - O)$. For all $Q \in E(K)$, $Q \neq P, O$,*

$$\{[P - O], [Q - O]\}_N{}^{|K^*|/N} = g_P(Q)^{|K^*|/N} \in K^*.$$

Proof. Taking a power of the Tate-pairing gives a non-degenerate pairing with values in K^* instead of K^*/K^{*N}. We give a different proof to show that the point O in $Q - O$ can be ignored. Let t_O be a k-rational local parameter for O, i.e. t_O vanishes to the order one in O. We may assume that $(t_O) \cap P = \emptyset$. Thus $Q - O + (t_O) \sim Q - O$, such that $Q - O + (t_O) \cap P - O = \emptyset$. With the following lemma, $g_P(Q - O + (t_O)) = g_P(Q) \in K^*/K^{*N}$. $\square$

Lemma 1 *Let $N = |E(k)|$. For a F-rational function f and for a F-rational divisor E such that $(f) \cap E = \emptyset$,*

$$f(E) = 1 \in K^*/K^{*N}.$$

Proof. We have $f(E) \in F^*$. The group order N is an odd divisor of $3^{3n} + 1$. Therefore, the group order N is coprime to $3^{3n} - 1$. And $F^* = F^{*N} \subset K^{*N}$. $\square$

Definition 1 ([V01],[BKLS02]) *Let $\rho \in F_{3^3}$ be a root of $\rho^3 - \rho - b = 0$. Let $\sigma \in F_{3^2}$ be a root of $\sigma^2 + 1 = 0$. Define the distortion map*

$$\phi : E(K) \to E(K), \quad \phi(x, y) = (\rho - x, \sigma y). \tag{1}$$

Combine the distortion map with Theorem 2 to obtain a pairing

$$E(k) \times E(k) \longrightarrow K^*, \quad (P, Q) \mapsto g_P(\phi(Q))^{|K^*|/N} \in K^*. \tag{2}$$

The curve $y^2 = x^3 - x + b$ has complex multiplication by -1 and the distortion map corresponds to multiplication by $\sqrt{-1}$. Indeed, ϕ is an automorphism of E,

$$(\sigma y)^2 = -y^2 = -x^3 + x - b = (\rho - x)^3 - (\rho - x) + b.$$

And $\phi^2 = -1$. The following remark is used in Theorem 3 [BKLS02] to discard contributions of the form $l_{P,O}(\phi(Q))$ in the evaluation of the Tate-pairing.

Algorithm 3 $E/k : y^2 = x^3 - x + b$ [BKLS02]

INPUT: $P \in E(k), Q = (x, y) \in F \times K, a = 3^{2m-1} \pm 3^m + 1.$

$\{[k : F_3] = 2m - 1, [F : k] = 3, [K : k] = 6, a = |E(k)|.\}$

OUTPUT: $f_a(Q) \in K^*/F^*$

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (l_{A,B}) = A + B + (-A - B) - 3O.\}$

$V \leftarrow P,\ a \leftarrow 1,\ f \leftarrow 1$
for $i = 1$ to $m - 1$ **do**
  $g \leftarrow l_{V,V} l_{V,-3V}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g\ \{a = 3, \ldots, 3^{m-1}\}$
end for
$g \leftarrow l_{\pm P,V}(Q)$
$a \leftarrow a \pm 1,\ V \leftarrow V \pm P,\ f \leftarrow f \cdot g\ \{a = 3^{m-1} \pm 1\}$
for $i = 1$ to m **do**
  $g \leftarrow l_{V,V} l_{V,-3V}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g\ \{a = 3^m + 3, \ldots, 3^{2m-1} \pm 3^m\}$
end for
$g \leftarrow l_{P,V}(Q)$
$a \leftarrow a + 1,\ V \leftarrow V + P,\ f \leftarrow f \cdot g\ \{a = 3^{2m-1} \pm 3^m + 1\}$

Remark 1 *Let $P \in E(k)$, $Q \in F \times K$, and let $l_{P,O}$ be the vertical line through P. Then $l_{P,O}(\phi(Q)) = 1 \in K^*/K^{*N}$.*

We point out some of the differences between Algorithm 2 and Algorithm 3.

1. The distortion map gives a non-degenerate pairing on $E(k) \times E(k)$.

2. Because of the simple ternary expension of N, a single loop of length $2m-1$ containing an if statement for the adding can be replaced with two smaller loops each followed by an unconditional addition.

3. The denominators in $l_{V,V}/l_{2V,O} \cdot l_{V,2V}/l_{3V,O}$ are omitted. Following Remark 1, they do not affect the value of the Tate-pairing.

4. The line $l_{V,2V}$ is written $l_{V,-3V}$. Since the line through $V, 2V$ and the line through $V, -3V$ are the same, the expressions are the same, but $-3V$ is easier to compute than $2V$. For $V = (\alpha, \beta)$, $-3V = (\alpha^9 - b, \beta^9)$.

For a further analysis of Algorithm 3 we refer to Appendix A.

5 The curve $C^d : y^2 = x^p - x + d$

Let C^d/k be the hyperelliptic curve $y^2 = x^p - x + d$, $d = \pm 1$, for $p \equiv 3 \pmod 4$. We assume that k is of degree $[k : F_p] = n$, for $\gcd(2p, n) = 1$, and we let F/k and K/k be the extensions of degree $[F : k] = p$ and degree $[K : k] = 2p$, respectively. Thus C^d is a direct generalization of the elliptic curve E^b studied in the previous sections. Over the extension field K, the curve is the quotient of a hermitian curve, hence is Hasse-Weil maximal. And the class group over K is annihilated by $p^{pn} + 1$. The last fact can be seen also from the following lemma. It shows that for $P \in C^d(K)$, $(p^{pn}+1)(P-O)$ is principal. We write $x^{(i)}$ for x^{p^i}.

Lemma 2 ([D96],[DS98]) *Let $P = (\alpha, \beta) \in C^d$. The function*

$$h_P = \beta^p y - (\alpha^p - x + d)^{(p+1)/2}$$

has divisor $(h_V) = p(V) + (V') - (p+1)O$, where

$$V' = (\alpha^{(2)} + d^p + d, \beta^{(2)}).$$

We will write V also for the divisor class $V - O$, so that $V' = -pV$. In particular $p^{pn}P = -P$, for $P \in C(K)$ and for $\mathrm{Trace}_{K/F_p} d = 0$. Let $M = p^{pn} + 1 = |K^*|/|F^*|$. Thus, the order of $P - O$ in the divisor class group Γ is a divisor of M. The precise order N of the class group can be obtained from the zeta functions for C^d in [D96], [DS98]. We will only need the following lemma.

Lemma 3 ([D96, Proposition 4.4]) *Let Γ^d denote the class group of the curve C^d/k, $d = \pm 1$.*

$$|\Gamma^+(k)||\Gamma^-(k)| = (p^{pn} + 1)/(p^n + 1)$$

In particular, $N = |\Gamma(k)|$ is an odd divisor of $M = p^{pn} + 1$.

We include the size of the class group for $p = 7$. Let $[k : F_7] = n$ and $m = (n + 1)/2$. Then

$$|\Gamma^+(k)| = (1 + 7^n)^3 + (\frac{7}{n})7^m(1 + 7^n + 7^{2n}).$$
$$|\Gamma^-(k)| = (1 + 7^n)^3 - (\frac{7}{n})7^m(1 + 7^n + 7^{2n}).$$

And $|\Gamma^+(k)||\Gamma^-(k)| = (1 + 7^{7n})/(1 + 7^n)$.

6 Main theorem

Miller's algorithm for the Tate-pairing on an elliptic curve E/k uses lines as building blocks to construct other rational functions. In our version of the Tate-pairing implementation, we will not rely on lines but on the functions described in Lemma 2. So that we can generalize from elliptic curves $E^b/k : y^2 = x^3 - x + b$, $b = \pm 1$, to hyperelliptic curves $C^d/k : y^2 = x^p - x + d$, $d = \pm 1$, for $p \equiv 3 \pmod 4$. Generalization of the results in Section 4 poses no problem.

Theorem 3 *Let $N = |\Gamma(k)|$, so that N divides $M = p^{pn} + 1 = |K^*|/|F^*|$. Let $P, O \in C(k)$ be distinct points. Let f_P be a k-rational function with $(f_P) = M(P - O)$. For all $Q \in E(K)$, $Q \neq P, O$,*

$$\{[P - O], [Q - O]\}_N{}^{|K^*|/N} = f_P(Q)^{|F^*|} \in K^*.$$

Proof. The argument that shows that the contribution by O can be omitted is the same as in Theorem 2. □

The difference with Theorem 2 is that f_P is computed with a multiple M of N instead of with N itself. The multiple M has trivial expansion in base p and this leads to Algorithm 4 which has no logical decisions (only point multiplication by p and no adding). This can be seen as an extreme case of an exponent of low Hamming weight [GHS02, Section 6]. Algorithm 4 has pn iterations compared to n iterations in Algorithm 3 (for the case $p = 3$). After Theorem 4, we will reduce this to n iterations in Algorithm 5. The following generalizations of Lemma 1 and Remark 1 are straighforward.

Lemma 4 *Let $N = |\Gamma(k)|$. For a F-rational function f and for a F-rational divisor E such that $(f) \cap E = \emptyset$,*

$$f(E) = 1 \in K^*/{K^*}^N.$$

Proof. We have $f(E) \in F^*$. The group order N is an odd divisor of $p^{pn} + 1$. Therefore, the group order N is coprime to $p^{pn} - 1$. And $F^* = {F^*}^N \subset {K^*}^N$. □

Remark 2 *Let $P \in E(F)$, $Q \in F \times K$, and let $l_{P,O}$ be the vertical line through P. Then $l_{P,O}(\phi(Q)) = 1 \in K^*/{K^*}^N$.*

Algorithm 4 $C/k : y^2 = x^p - x + d.$

INPUT: $P \in E(k), Q \in F \times K, a = p^{pn} + 1$

$\{[k : F_p] = n, [F : k] = p, [K : k] = 2p, a = |K^*|/|F^*|.\}$

OUTPUT: $f_a(Q) \in K^*/F^*$

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (h_V) = p(V) + (-pV) - (p+1)O.\}$

$V \leftarrow P$, $a \leftarrow 1$, $n \leftarrow 1$, $d \leftarrow 1$
for $i = 1$ to pn **do**
  $g \leftarrow h_V(Q)$
  $a \leftarrow pa$, $V \leftarrow pV$, $f \leftarrow f^p \cdot g$
end for

Definition 2 *Let $\rho \in F$ be a root of $\rho^p - \rho + 2d = 0$. Let $\sigma \in K$ be a root of $\sigma^2 + 1 = 0$. Define the distortion map*

$$\phi : C(K) \to C(K), \quad \phi(x, y) = (\rho - x, \sigma y). \tag{3}$$

Combine the distortion map with Theorem 3 to obtain a map

$$C(k) \times C(k) \longrightarrow K^*, \quad (P, Q) \mapsto f_P(\phi(Q))^{|F^*|} \in K^*. \tag{4}$$

Indeed, $(\sigma y)^2 = -y^2 = -x^p + x - d = (\rho - x)^p - (\rho - x) + d$.

Theorem 4 (Main Theorem) *For $P = (\alpha, \beta), Q = (x, y) \in C(k)$,*

$$f_P(\phi(Q)) = \prod_{i=1}^{n} \left(\beta^{(i)} y^{(n+1-i)} \bar{\sigma} - (\alpha^{(i)} + x^{(n+1-i)} - \rho + d)^{(p+1)/2}\right).$$

Proof. From Algorithm 4, we see that

$$f_P(\phi(Q)) = \prod_{i=1}^{pn} (h_{p^{i-1}P}(\phi(Q))^{(pn-i)}$$

Substitution of

$$\begin{aligned} h_P(Q) &= \beta^p y - (\alpha^p - x + d)^{(p+1)/2} \\ p^{i-1}P &= (\alpha^{(2i-2)} + (i-1)2d, (-1)^{i-1}\beta^{(2i-2)}) \\ \phi(Q) &= (\rho - x, \sigma y) \end{aligned}$$

yields

$$\begin{aligned} &\prod_{i=1}^{pn} \left((-1)^{i-1}\beta^{(2i-1)}(\sigma y) - (\alpha^{(2i-1)} + (i-1)2d - (\rho - x) + d)^{(p+1)/2}\right)^{(pn-i)} \\ &= \prod_{i=1}^{pn} \left((-1)^{i-1}\beta^{(i-1)}\sigma^{(pn-i)} y^{(pn-i)}\right. \\ &\qquad \left. - (\alpha^{(i-1)} + (i-1)2d - (\rho - (pn-i)2d - x^{(pn-i)}) + d)^{(p+1)/2}\right). \end{aligned}$$

Or, since $\alpha, \beta, x, y \in k$, and since $(-1)^{i-1}\sigma^{(pn-i)} = \sigma$, for both i odd and i even,

$$\begin{aligned} &\prod_{i=1}^{n} \left(\beta^{(i-1)} y^{(n-i)} \sigma - (\alpha^{(i-1)} - \rho + x^{(n-i)} - d)^{(p+1)/2}\right)^p \\ &= \prod_{i=1}^{n} \left(\beta^{(i)} y^{(n+1-i)} \bar{\sigma} - (\alpha^{(i)} + x^{(n+1-i)} - \rho^p - d)^{(p+1)/2}\right). \end{aligned}$$

Finally, $-\rho^p - d = -\rho + d$. $\square$

Algorithm 5 $C/k : y^2 = x^p - x + d$.

INPUT: $P = (\alpha, \beta) \in E(k)$, $Q = (\rho - x, \sigma y), (x, y) \in E(k)$, $a = p^{pn} + 1$

$\{[k : F_p] = n, \rho^p - \rho + 2d = 0, \sigma^2 + 1 = 0.\}$

$\{[F : F_p] = pn, [K : F_n] = 2pn, a = |K^*|/|F^*|.\}$

OUTPUT: $f_a(Q) \in K^*/F^*$

$\{(f_a) = a(P) - (aP) - (a-1).\}$

for $i = 1$ to n **do**
  $\alpha \leftarrow \alpha^{(1)}, \beta \leftarrow \beta^{(1)}$
  $g \leftarrow (\beta y \bar{\sigma} - (\alpha + x - \rho + d)^{(p+1)/2})$
  $f \leftarrow f \cdot g$
  $x \leftarrow x^{(-1)}, y \leftarrow y^{(-1)}$
end for

Note the symmetry in P and Q: $f_P(\phi(Q)) = f_Q(\phi(P))$.

Summarizing, using a Tate-pairing $\{-,-\}_M$ instead of $\{-,-\}_N$ removes all logic and all additions from Algorithm 3. When using the version Algorithm 5, the number of iterations is similar to Algorithm 3. Using Algorithm 5 has the following advantages.

1. Uniform algorithm that applies to all $p \equiv 3 \pmod 4$.
2. Expressing $N = |\Gamma(k)|$ in base p can be omitted.
3. Expressing $|K^*|/N$ in base p, for raising $g_P(Q)$ to the power $|K^*|/N$, can be omitted.
4. At each iteration, only multiplication by p is required, no additions.
5. Multiplication by p using the function h_P is faster than using a product of lines (the case $p = 3$, see Appendix A).

7 The bilinear Diffie-Hellman problem

Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order q. We assume that the discrete log problem (DLP) in both G_1 and G_2 are hard. Let $e : G_1 \times G_1 \to G_2$ be a pairing which satisfies the following conditions.

(i) Bilinearity : $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$, and for all $a, b \in Z$.
(ii) Non-degeneracy : The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Observe that since G_1 and G_2 are groups of prime order this implies that if P is a generator of G_1, then $e(P, P)$ is a generator of G_2.
(iii) Computability : Given $P, Q \in G_1$, $e(P, Q)$ can be computed efficiently.

A bilinear map satisfying the three properties above is said to be an *admissible bilinear map*. We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps. We refer to [BF01], [V01] for more details.

Bilinear Diffie-Hellman Problem : Let $e : G_1 \times G_1 \to G_2$ be an admissible bilinear map defined as above. Let P be a generator of G_1. The BDH problem in $< G_1, G_2, e >$ is as follows. Given $P, aP, bP, cP \in G_1$, compute $e(P, P)^{abc} \in G_2$ where a, b, c are randomly chosen from Z_q^*. A randomized algorithm $\mathcal{A}$ is said to solve the BDH problem with an advantage of ϵ if

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}] \geq \epsilon.$$

where the probability is over the random choices of a, b, c in ${Z_q}^*$, the random choice of $P \in G_1^*$, and the random bits of $\mathcal{A}$.

Bilinear Diffie-Hellman Assumption : We assume that the BDH problem is hard, which means there is no polynomial time algorithm to solve the BDH problem with non-negligible probability.

Now we introduce Joux's tripartite Diffie-Hellman (TDH) protocol from admissible bilinear pairings.

Joux's Tripartite Diffie-Hellman(TDH) Protocol : Assume A, B and C want to share a common secret.

Protocol messages :
$A \to B, C : aP$
$B \to A, C : bP$
$C \to A, B : cP$

In the protocol, " $\to$ " is denoted by *broadcast* (or *send*) to the others. Once the communication is over, A computes $K_A = e(bP, cP)^a$, B computes $K_B = e(aP, cP)^b$ and C computes $K_C = e(aP, bP)^c$. By bilinearity of e, these are all equal to $K = e(P,P)^{abc}$ and K is the secret key shared by A, B and C.

The security of this protocol is based on the hardness of the bilinear Diffie-Hellman problem.

By *a single pass of communication* (or *a one round communication*), we mean that each participant is allowed to talk once and broadcast some data to the others. The step of *round zero* means that each participant chooses a random private key and broadcasts a public key to the others. The situation where three or more parties share a secret key is getting more important as group communications on open networks are increasing. Therefore there have been many attempts to extend the well-known two-party Diffie-Hellman key exchange protocol [DH76] to the multi-party setting [BD95], [STW96], [AST98], [BW98], [BS02]. In the following section, we present an n-round key agreement protocol for any N-participants, where $3^{n-1} < N \leq 3^n$, $n > 1$. The case of $N = 3$ is done by Joux's one round protocol [J00].

8 A group key agreement protocol

We assume that N participants want to share a common secret, for $3^{n-1} < N \leq 3^n$, $n > 1$. We present an n-round key agreement protocol for any N-parties. First we give a two-round key agreement protocol for nine participants.

Example. *Two round key agreement protocol for nine participants* :

• Round 0 (Preparation) : Let $A_1, A_2, \cdots, A_9$ be the participants who want to share a common secret. Each A_i chooses a random secret number a_i, computes a_iP and broadcasts this public value. Let $h : G_2 \to (Z/q)^*$ be a hash function.

• Round 1 : Each participant A_i in the subgroup X_1, X_2 or X_3 computes a common sub-key as follows.
$X_1 = \{A_1, A_2, A_3\}$ computes $K_1 = e(P,P)^{a_1a_2a_3}$.
$X_2 = \{A_4, A_5, A_6\}$ computes $K_2 = e(P,P)^{a_4a_5a_6}$.
$X_3 = \{A_7, A_8, A_9\}$ computes $K_3 = e(P,P)^{a_7a_8a_9}$.
Each member in X_1, X_2 and X_3 computes $h(K_1) = c_1$, $h(K_2) = c_2$ and $h(K_3) = c_3$, respectively. Then c_1, c_2 and c_3 are the shared sub-keys for members belonging to the class X_1, X_2 and X_3, respectively. Let the user with the smallest index be a representative of each class. Then A_1, A_4 and A_7,

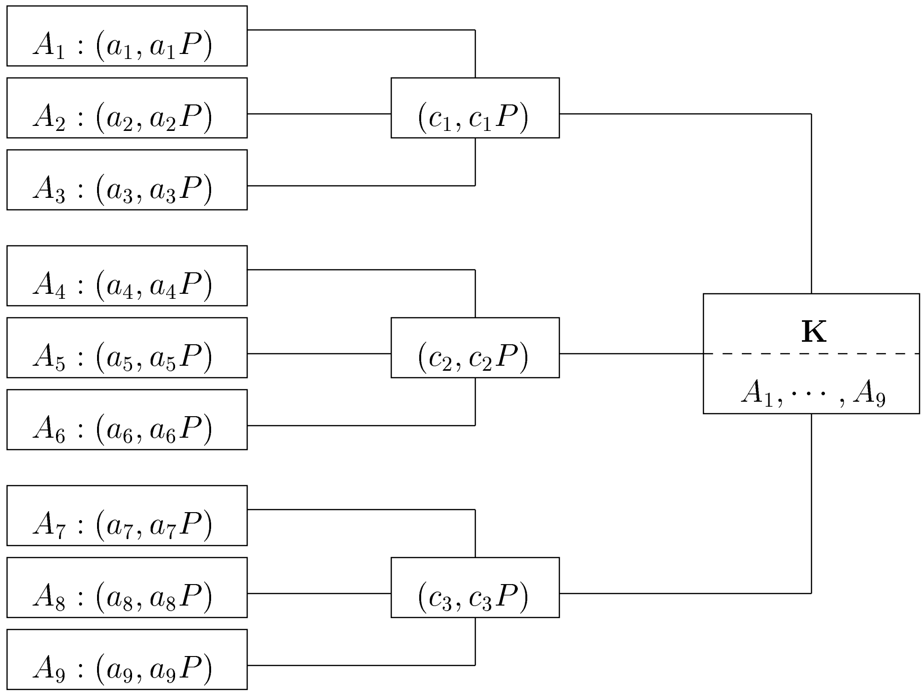

Figure 1. Two-round nine-party key agreement.

as representatives of X_1, X_2 and X_3, compute c_1P, c_2P and c_3P, respectively, and broadcast these public values.
• Finally : Each participant A_i computes the common secret key, using his shared sub-key and other public values,

$$K = e(c_1P, c_2P)^{c_3} = e(c_1P, c_3P)^{c_2} = e(c_2P, c_3P)^{c_1} = e(P, P)^{c_1c_2c_3}$$

Therefore all A_i obtain the shared common secret K (See Figure 1.)

Next we provide an n-round group key agreement protocol for $N = 3^n,\ n > 1$, and then describe the protocol for any N, where $3^{n-1} < N \leq 3^n,\ n > 1$.

Notation :
Let the participants be divided over classes such that all members of a given class share a common public value. Let N_i be the number of such classes at the beginning of round i. In particular $N_1 = N$.
Let $\ulcorner N_i/3 \urcorner$ = maximum integer less than $N_i/3 + 1$.

Protocol for $\mathbf{N = 3^n,\ n > 1}$.

Protocol 1. n-round key agreement protocol for N parties, $N = 3^n,\ n > 1$.

Round 0 (Setup) : Let $A_1, \cdots, A_N$ be the participants who want to share a common secret. Each A_i chooses a random secret number a_i, computes a_iP and broadcasts this public value. Let $h : G_2 \to (Z/q)^*$ be a hash function.

Round i, $(1 \le i \le n-1)$:

Divide the N_i classes over $N_{i+1} = N_i/3$ classes. Each class j, for $j = 1, 2, \ldots, N_{i+1}$, consists of three subclasses with three different public values. The members in class j compute the common sub-key $K_{i,j} = e(P,P)^{\alpha_{j1}\alpha_{j2}\alpha_{j3}}$, where $\alpha_{j1}P, \alpha_{j2}P$ and $\alpha_{j3}P$ are the public values of the three subclasses in class j. Each member of the class j computes $h(K_{i,j}) = c_{ij} \in (Z/q)^*$ and a representative of each class, say A_l ($l \equiv 1 \bmod 3^i$), computes $c_{ij}P$ and broadcasts this as a class public value.

Finally : Each participant computes the shared group secret

$$K_{n,1} = e(P,P)^{c_{n-1,1}c_{n-1,2}c_{n-1,3}}$$

using TDH based on private values $c_{n-1,1}, c_{n-1,2}, c_{n-1,3}$ and public values $c_{n-1,1}P$, $c_{n-1,2}P$, $c_{n-1,3}P$.

Protocol 1 is the special case of the following protocol 2.

Protocol for N, where $\mathbf{3^{n-1} < N \le 3^n,\ n > 1}$.

Protocol 2. n-round key agreement protocol for any N parties, $3^{n-1} < N \le 3^n,\ n > 1$.

Round 0 (Setup) : Let $A_1, \cdots, A_N$ be the participants who want to share a common secret. Each A_i chooses a random secret number a_i, computes a_iP and broadcasts this public value. Let $h : G_2 \to (Z/q)^*$ be a hash function.

Round i, $(1 \le i \le n-1)$:

(case 1) $N_i - 3^{n-i} \equiv 0 \pmod 3$
This step is the same as Round i in Protocol 1.

(case 2) $N_i - 3^{n-i} \equiv 1 \pmod 3$
Divide the group N_i into $N_{i+1} = \ulcorner N_i/3 \urcorner$ classes. Each class j, for $j = 1, 2, \ldots, N_{i+1} - 1$, consists of three subclasses with three different public values. The members in class j compute the common sub-key $K_{i,j} = e(P,P)^{\alpha_{j1}\alpha_{j2}\alpha_{j3}}$, where $\alpha_{j1}P, \alpha_{j2}P$ and $\alpha_{j3}P$ are the public values of the three subclasses in

class j. The last class N_{i+1} keeps its previous public value. Each member of the class j, for $j = 1, 2, \ldots, N_{i+1}$, computes $h(K_{i,j}) = c_{ij} \in (Z/q)^*$ and a representative of each class, say A_l ($l \equiv 1 \bmod 3^i$), computes $c_{ij}P$ and broadcasts this as a class public value.

(case 3) $N_i - 3^{n-i} \equiv 2 \pmod 3$
Divide the group N_i into $N_{i+1} = \ulcorner N_i/3 \urcorner$ classes. Each class j, for $j = 1, 2, \ldots, N_{i+1} - 1$, consists of three subclasses with three different public values. The members in class j compute the common sub-key $K_{i,j} = e(P,P)^{\alpha_{j1}\alpha_{j2}\alpha_{j3}}$, where $\alpha_{j1}P, \alpha_{j2}P$ and $\alpha_{j3}P$ are the public values of the three subclasses in class j. The last class N_{i+1} computes $K_{i,N_{i+1}} = \alpha_{N_{i+1},1}\alpha_{N_{i+1},2}P$ using a 2-party Diffie-Hellman protocol. Each member of the class j, for $j = 1, 2, \ldots, N_{i+1}$, computes $h(K_{i,j}) = c_{ij} \in (Z/q)^*$ and a representative of each class, say A_l ($l \equiv 1 \bmod 3^i$), computes $c_{ij}P$ and broadcasts this as a class public value.

Finally : After Round $n-1$, the number of classes N_n is either 3 or 2, since $N > 3^{n-1}$. Therefore each participant computes the shared group secret key $K_{n,1} = e(P,P)^{c_{n-1,1}c_{n-1,2}c_{n-1,3}}$ using TDH or $K_{n,1} = c_{n-1,1}c_{n-1,2}P$ using DH based on the secret value for its class and the public values of the other classes.

A A closed formula for the BKLS-Algorithm

Let $E^b/k : y^2 = x^3 - x + b$ be an elliptic curve as in Section 3. Recall from Definition 1 in Section 4 the pairing $E(k) \times E(k) \longrightarrow K^*$,

$$(P, Q) \mapsto g_P(\phi(Q))^{|K^*|/N} \in K^*.$$

For the efficient evaluation of $g_P(\phi(Q))$ we follow Algorithm 3.

Remark 3 We make three remarks. They all reflect that the lines that are computed by the algorithm can be precomputed.

1. After the first loop, we have, for $P = (\alpha^3, \beta^3)$,

$$l_{\pm P,V} = \pm y - \beta(x - \alpha + b).$$

2. After the second loop $V = (3^{2m-1} \pm 3^m)P = -P$, and multiplication by $l_{P,-P}(Q) = l_{P,0}(Q)$ can be omitted.

3. Inside each loop, if we omit only the denominator $l_{3V,O}$, we find

$$(l_{V,V}l_{V,-3V}/l_{2V,O}) = 3V + (-3V) - 4O.$$

For $V = (\alpha, \beta)$, the function $h_V : \beta^3 y - (\alpha^3 - x + b)^2$ has the same divisor. We claim that using h_V in place of $l_{V,V}l_{V,-3V}$ uses fewer operations.

Theorem 5 (Algorithm 3 in closed form) *Let*

$$P = (\alpha^3, \beta^3) \in E(k), \quad Q = (x, y) \in E(k), \quad \phi(Q) = (\rho - x, \sigma y).$$

Then, for g_P with $(g_P) = N(P - Q)$, $g_P(\phi(Q))$ is the product of

$$\begin{aligned}
&\prod_{i=1}^{m-1} \left(\beta^{(i)} y^{(n-i)} \sigma - (\alpha^{(i)} + x^{(n-i)} - \rho + mb)^2\right), \\
&\prod_{i=m}^{2m-1} \left(\beta^{(i)} y^{(n-i)} \sigma - (\alpha^{(i)} + x^{(n-i)} - \rho - b)^2\right), \\
&(\pm \sigma y - \beta(\rho - x - \alpha + b))^{(m)}.
\end{aligned}$$

The second remark is clear. In the remainder of this section we first prove the third remark, then the first remark and finally the theorem.

Lemma 5 *Let $l_{A,B}$ be the line through A and B. For $V = (\alpha, \beta) \in E(K)$,*

$$\begin{aligned}
&l_{V,V} : (x - \alpha) - \beta(y - \beta) = 0, \\
&l_{2V,O} : x - \alpha - 1/\beta^2 = 0, \\
&l_{2V,V} : (\beta^4 - 1)(x - \alpha) - \beta(y - \beta) = 0, \\
&l_{3V,O} : x - \alpha^9 + b = 0.
\end{aligned}$$

The lines $l_{V,V}, l_{2V,V}$ correspond to l_1 and l'_1, respectively, in [GHS02], up to a slight difference to reduce the number of operations. For the third remark, we compare the number of operations (Multiplication, Squaring, Addition, Frobenius).

$$\begin{array}{ll}
g \leftarrow l_{V,V}l_{V,-3V},\, f \leftarrow f^3 \cdot g & \text{(4M,4A,1F)} \\
g \leftarrow h_V,\, f \leftarrow f^3 \cdot g & \text{(2M,1S,2A,1F)}
\end{array}$$

To establish the first remark we use the following lemma.

Lemma 6 *Let $(\alpha,\beta) \in E^b(\bar{F}_3)$. The line $l : by - \beta(x-\alpha+b) = 0$ has divisor*

$$(\alpha,\beta) \ + \ (\alpha+b,-\beta) \ + \ (\alpha^3, b\beta^3) \ - \ 3O.$$

Let $(\alpha,\beta) \in E^b(k)$, for k of degree $[k:F_3] = n = 2m-1$ with $\gcd(6,n)=1$.

$$\begin{array}{lll} n = 1(3): & 3^n(\alpha+b,-\beta) = (\alpha,\beta), & 3^m(\alpha+b,-\beta) = (\alpha^3,(-1)^{m+1}\beta^3). \\ n = 2(3): & 3^n(\alpha,\beta) = (\alpha+b,-\beta), & 3^m(\alpha,\beta) = (\alpha^3,(-1)^m\beta^3). \end{array}$$

Proof. The first claim is obvious. The last claim uses

$$V = (\alpha,\beta) \Rightarrow 3V = (\alpha^9 - b, -\beta^9)$$

□

We summarize in a table.

	$n=1(3), m=1(3)$	$n=2(3), m=0(3)$
(α,β)	3^nW	W
$(\alpha+b,-\beta)$	W	3^nW
$(\alpha^3,b\beta^3)$	$\varepsilon 3^mW$	$\varepsilon 3^mW$
ε	$(-1)^{m+1}b$	$(-1)^mb$

With the value for ε from the table, $E(k) = 3^n + 1 + \varepsilon 3^m$.

Proposition 1 *Let $P = (\alpha^3,\beta^3) \in E^b(k)$, for k of degree $[k:F_3] = n = 2m-1$ with* $\gcd(6,n)=1$. *The line through εP and $V = 3^{m-1}P$ has equation*

$$l_{\varepsilon P,V} : \varepsilon y - \beta(x-\alpha+b) = 0.$$

The third point on the line $l_{\varepsilon P,V}$ is $(\alpha+mb,(-1)^m\beta)$.

Proof. We apply the lemma. Write $P = 3^mW$, so that $V = 3^nW$. The line through $\varepsilon P = (\alpha^3,\varepsilon\beta^3)$ and V follows from the lemma. The lemma also shows that W is the third point on the line. And W can be obtained from the table, or alternatively as the unique point W with $3^mW = P$. □

This proves the first remark. We can now prove Theorem 5. The contribution of the first loop to $g_P(\phi(Q))$ is

$$\begin{aligned}
&\prod_{i=1}^{m-1} \left((-1)^{i-1}\beta^{(2i)}(\sigma y) - (\alpha^{(2i)} - (i-1)b - (\rho - x) + b)^2\right)^{(2m-1-i)} \\
&= \prod_{i=1}^{m-1} \Big((-1)^{i-1}\beta^{(i)}\sigma^{(n-i)}y^{(n-i)} \\
&\qquad -(\alpha^{(i)} - (i-1)b - (\rho + (2m-1-i)b - x^{(n-i)}) + b)^2\Big) \\
&= \prod_{i=1}^{m-1} \left(\beta^{(i)}y^{(n-i)}\sigma - (\alpha^{(i)} + x^{(n-i)} - \rho + mb)^2\right).
\end{aligned}$$

The second loop starts with $V = (\alpha + mb, (-1)^{m+1}\beta)$ instead of $V = P = (\alpha^3, \beta^3)$ and is of length m instead of length $m-1$. It gives a contribution

$$\begin{aligned}
&\prod_{i=1}^{m} \left((-1)^{i+m}\beta^{(2i-1)}(\sigma y) - (\alpha^{(2i-1)} + (m+1-i)b - (\rho - x) + b)^2\right)^{(m-i)} \\
&= \prod_{i=1}^{m} \Big((-1)^{i+m}\beta^{(m-1+i)}\sigma^{(m-i)}y^{(m-i)} \\
&\qquad -(\alpha^{(m-1+i)} + (m+1-i)b - (\rho + (m-i)b - x^{(m-i)}) + b)^2\Big) \\
&= \prod_{i=m}^{2m-1} \left(\beta^{(i)}y^{(n-i)}\sigma - (\alpha^{(i)} + x^{(n-i)} - \rho - b)^2\right).
\end{aligned}$$

The contribution from $l_{\varepsilon P,V}$ follows directly from the proposition. This proves Theorem 5. $\square$

References

[AST98] G. Atenies, M. Steiner, G. Tsudik, "Authenticated group key agreement and friends." ACM Conference on Computer and Communications Security, (1998).

[PBCL] The Pairing-Based Crypto Lounge, http://planeta.terra.com.br/informatica/paulobarreto/pblounge .html

[BKLS02] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science 2442, Springer-Verlag (2002), pp. 354–368. See also Cryptology ePrint Archive, Report 2002/008

[BW98] C. Becker and U. Willie, "Communication complexity of group key distribution." ACM conference on Computer and Communication Society, (1998).

[BSS99] I. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography. London Mathematical Society LNS, 265. Cambridge University Press, Cambridge, 1999 (reprinted 2000).

[BF01] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing." Advances in Cryptology, Crypto 2001, Springer-Verlag, (2001).

[BS02] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography," To appear in Contemporary Mathematics, American Mathematical Society. See also Cryptology ePrint Archive: Report 2002/080.

[BD95] M. Burmester and Y. Desmedt. A Secure and efficient Conference key Distribution System, Advances in Cryptology-Eurocrypto'94, LNCS, Springer Verlag, 275-286, (1995).

[CC03] J. C. Cha, J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," International Workshop on Practice and Theory in Public Key Cryptography – PKC'2003, to appear.

[DH76] W. Diffie and M. Hellman. "New direction in cryptography," IEEE Trans. Information Theory, IT-22(6):644-654, (1976).

[D96] I. Duursma, "Class numbers for some hyperelliptic curves." In: "Arithmetic, Geometry and Coding Theory," eds. Pellikaan, Perret, Vladuts, pp.45-52, publ. deGruyter, Berlin, 1996.

[DS98] I. Duursma, K. Sakurai, "Efficient algorithms for the Jacobian variety of hyperelliptic curves $y^2 = x^p - x + 1$ over a finite field of odd characteristic p." Coding theory, cryptography and related areas (Guanajuato, 1998), 73–89, Springer, Berlin, 2000.

[FR94] G. Frey, H.-G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves." Math. Comp. 62 (1994), no. 206, 865–874.

[G01] S.D. Galbraith, "Supersingular curves in cryptography." Asiscrypt (2001), Springer LNCS 2248, 495–513.

[GHS02] S. D. Galbraith, K. Harrison, D. Soldera, "Implementing the Tate pairing," Algorithmic Number Theory Symposium – ANTS-V, Lecture Notes in Computer Science 2369, Springer-Verlag (2002), pp. 324–337.

[H02a] F. Hess, Exponent group signature schemes and efficient identity based signature schems based on pairing, Proceedings of the Workshop Selected Areas in Cryptology, SAC, Aug. 2002.

[H02b] F. Hess, "A Note on the Tate Pairing of Curves over Finite Fields," 2002. Available on http://www.math.tu-berlin.de/ hess.

[IT02] T. Izu and T. Takagi, "Efficient Computations of the Tate Pairing for the Large MOV degrees." 5th International Conference on Information Security and Cryptology, ICISC 2002, Springer-Verlag, to appear.

[J00] A. Joux, "A one round protocol for tripartite Diffie-Hellman," Proceedings of Algorithmic Number Theory Symposium, vol 1838, LNCS, Springer-Verlag, 385-394, (2000).

[K98] N. Koblitz, "An elliptic curve implementation of the finite field digital signature algorithm." Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), 327–337, Lecture Notes in Comput. Sci., 1462, Springer, Berlin, 1998.

[M86] V. Miller, "Short Programs for Functions on Curves," Unpublished manuscript, 1986.

[MOV93] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Transactions on Information Theory 39 (1993), pp. 1639–1646.

[P02] K.G. Paterson, “ID-based signature from pairings on elliptic curves.” Electronics Letters, Vol. 38 (18) (2002), 1025-1026.

[SOK00] R. Sakai, K. Ohgishi and M. Kasahara, ”Cryptosystems based on pairing.” Symposium on cryptography and Information Security, Okinawa, Japan, pp. 26-28, (2000)

[S02] N.P. Smart, “An identity based authentication key agreement protocol based on pairing.” Electronics Letters, Vol 38, pp 630-632, (2002).

[STW96] M. Stein, G. Tsudik, M. Waidner, “Diffie Hellman Key Distribution extended to group communication.” ACM conference on computer and communication security, (1996).

[V01] E. Verheul, “Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.” Advances in cryptology—EUROCRYPT ’2001, 195–210, Lecture Notes in Comput. Sci., 2045, Springer, Berlin, 2001.