Designs, Codes and Cryptography, 37, 133–141, 2005

Elliptic Curves Suitable for Pairing Based Cryptography

FRIEDERIKE BREZING brezing@stud.uni-frankfurt.de
Fachbereich Mathematik, Johann Wolfgang Goethe-Universität, Robert-Mayer-Str. 10, 60051 Frankfurt, Germany

ANNEGRET WENG weng@mathematik.uni-mainz.de
Fachbereich Mathematik, Johannes Gutenberg Universität, Staudingerweg 9, 55128 Mainz, Germany

Communicated by: A. Menezes

Received September 19, 2003, Revised June 17, 2004; Accepted September 13, 2004

Abstract. For pairing based cryptography we need elliptic curves defined over finite fields $\mathbb{F}_q$ whose group order is divisible by some prime ℓ with $\ell \mid q^k - 1$ where k is relatively small. In Barreto et al. and Dupont et al. [Proceedings of the Third Workshop on Security in Communication Networks (SCN 2002), LNCS, 2576, 2003; Building curves with arbitrary small Mov degree over finite fields, Preprint, 2002], algorithms for the construction of ordinary elliptic curves over prime fields $\mathbb{F}_p$ with arbitrary embedding degree k are given. Unfortunately, p is of size $O(\ell^2)$.

We give a method to generate ordinary elliptic curves over prime fields with p significantly less than ℓ^2 which also works for arbitrary k. For a fixed embedding degree k, the new algorithm yields curves with $p \approx \ell^s$ where $s = 2 - 2/\varphi(k)$ or $s = 2 - 1/\varphi(k)$ depending on k. For special values of k even better results are obtained.

We present several examples. In particular, we found some curves where ℓ is a prime of small Hamming weight resp. with a small addition chain.

Keywords: elliptic curves, pairing based cryptagraphy

AMS Classification: 14H52, 14G50

1. Introduction

Over the last few years there has been an increasing interest in pairing based cryptography. The primitives of pairing based crypto systems are two groups $(G, *)$ and $(H, \circ)$ in which the discrete logarithm problem is believed to be hard. Moreover, we require the existence of an efficiently computable, non-degenerate pairing $G \times G \to H$. This additional structure allows many interesting protocols for all kind of different applications [5, 7, 10, 12].

Well known examples are the Weil and the Tate pairing on an elliptic curve. Here, G is the group of points on an elliptic curve defined over a finite field $\mathbb{F}_q$ and H is equal to the multiplicative group of a field extension $\mathbb{F}_{q^k}^*$.

Definition 1.1. Let E be an elliptic curve defined over $\mathbb{F}_q$ whose group order $\#E(\mathbb{F}_q)$ is divisible by a prime ℓ. Then E has **embedding degree** k **with respect to** ℓ if k is the smallest integer such that ℓ divides $q^k - 1$.

If E has embedding degree $k > 1$ with respect to ℓ, the Weil pairing e_ℓ defines a non-degenerate pairing from the group of ℓ- torsion points in $E(\mathbb{F}^*_{q^k})$ into $\mathbb{F}^*_{q^k}$. It can be evaluated in $O(k^2 \log^3 q)$ bit operations. Supersingular elliptic curves have embedding degree less than or equal to 6 [8,11].

It is an interesting question whether there exist suitable elliptic curves with $k \geq 7$. Obviously, they can not be supersingular. But ordinary elliptic curves with such a small embedding degree are very rare [2]. We are left with the problem to construct ordinary curves with relatively small embedding degree (see e.g. [3,6]).

Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and let ℓ be a prime dividing the group order $\#E(\mathbb{F}_q)$ such that E has embedding degree k with respect to ℓ. We have

$$\#E(\mathbb{F}_q) = q + 1 - t \equiv 0 \mod \ell \text{ and} \tag{1}$$

$$q^k - 1 \equiv 0 \mod \ell. \tag{2}$$

Inserting equation (2) in (1) shows that $(t-1)$ must be a k-th root of unity modulo ℓ. On the other hand, if E is an elliptic curve over $\mathbb{F}_q$ satisfying equation (1) and $t = \zeta_k + 1 \mod \ell$ for some primitive k-th roots of unity ζ_k modulo ℓ, E has embedding degree k with respect to ℓ. The relevance of this fact to pairing based cryptography was first pointed out by C. Cocks and R. Pinch.

Since E is ordinary, it has complex multiplication by some order $\mathcal{O}$ of discriminant dividing $t^2 - 4q$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ where $-d > 0$ is squarefree. From now on we assume that $\mathcal{O}$ is the maximal order in K.

The Frobenius element $\pi_q : (x, y) \to (x^q, y^q)$ corresponds to an element $w = \frac{a+b\sqrt{d}}{2} \in \mathcal{O}$ such that $\mathrm{Norm}_{K/\mathbb{Q}}(w) = w\overline{w} = q$. We have $t = a$.

This observation leads to a simple algorithm. Given an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$. Take a prime ℓ with the properties that ℓ splits in $\mathcal{O}$ and $\ell \equiv 1 \mod k$ and determine a primitive k-th root of unity ζ_k modulo ℓ. Set $a = \zeta_k + 1 \mod \ell$ and $b = \pm\frac{a-2}{\delta} \mod \ell$ where δ is a square root of d modulo ℓ. Finally test whether $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ with $w = \frac{a+b\sqrt{d}}{2}$ is a prime p (or a prime power q). We find the corresponding elliptic curve defined over $\mathbb{F}_p$ (or $\mathbb{F}_q$) using the complex multiplication method (for the CM method see e.g. [1]).

The correctness of this method can easily be seen by the following lemma which summarizes the discussion above.

LEMMA 1.1. *Let $E/\mathbb{F}_q$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{d})$ such that the Frobenius endomorphism corresponds to the imaginary quadratic integer $w = \frac{a+b\sqrt{d}}{2}$ with a, b constructed as above. Then $\#E(\mathbb{F}_q)$ is divisible by ℓ and has embedding degree k with respect to ℓ.*

Proof. By the choice of b, we find

$$\#E(\mathbb{F}_q) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(w-1) = \frac{1}{4}((a-2)^2 - db^2) \equiv 0 \mod \ell.$$

Since the trace t of π_q is equal to $a = \zeta_k + 1 \mod \ell$, the embedding degree of E with respect to ℓ is equal to k. ■

Note that the case that $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ is not a prime but a prime power is very unlikely. Hence in the following we only consider the case where $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ is prime.

The values a and b are solutions of equations modulo ℓ. Hence, they will in general be of size $O(\ell)$ leading to a prime of size $O(\ell^2)$. Desirable would be to have p of size $O(\ell)$, because the security of the cryptosystem based on the pairing will depend on the largest prime factor ℓ dividing the group order $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_p)$ is of size p.

It is still an open question to find an algorithm for the construction of ordinary elliptic curves with arbitrary embedding degree k where p is significantly smaller than ℓ^2. Barreto, Lynn and Scott describe a method to derive a better relation between p and ℓ for the case where k is divisible by 3 [3]. In this paper we extend their idea using the fact that E has embedding degree k if and only if $t-1$ is a k-th root of unity modulo ℓ and get more examples of curves with $p \in O(\ell^{2-\epsilon})$ for $\epsilon > 0$. Our method works for general k.

Moreover we find examples where ℓ is a prime of low Hamming weight with respect to the basis 2. For such primes, the Weil resp. Tate pairing can be efficiently evaluated [4,9].

2. The General Approach

Given k and a discriminant $D < 0$ which is not too large. Let d be the squarefree part of D, i.e. $d = D$ iff $D \equiv 1 \mod 4$ and $d = D/4$ otherwise. We can consider the number field $M(\zeta_n, \sqrt{d})$ for some n, $k \mid n$. Suppose $M \simeq \mathbb{Q}[x]/(f(x))$ where f is an irreducible polynomial of degree d_f where $d_f = 2\varphi(n)$ or $\varphi(n)$ depending on whether $\sqrt{d} \subseteq \mathbb{Q}(\zeta_n)$ or not. Additionally, we require that f represents primes.

Every element in M can be represented by a polynomial of degree $\leq d_f - 1$. We can compute the polynomials $g_1, \ldots, g_{\varphi(k)}$ which represent the primitive k-th roots of unity. Let $h_1, h_2 = -h_1$ be the polynomials which represent $\pm\sqrt{d}$. Suppose that g_i and h_i lie in $\mathbb{Z}[x]$.

We now set

$$a(x) = (g_i(x) + 1)$$

and

$$b'(x) = (a(x) - 2)h_j(x) \text{ in } \mathbb{Q}[x]/(f(x)).$$

for some $1 \leq i \leq \varphi(k)$, $1 \leq j \leq 2$.

We test if there exists some congruence class $x_0 \mod (-d)$ such that $b'(x_0) \equiv 0 \mod (-d)$. For all x_1 with $x_0 \equiv x_1 \mod (-d)$, $b'(x_1)/d$ will be an integer. Set

$$p(x) = \frac{1}{4}\left(a(x)^2 - \frac{b'(x)^2}{d}\right).$$

Now suppose the following conditions are satisfied:

- $p(x)$ is irreducible,
- $p(x)$ has integer values for $x_0 \mod (-d)$ and
- $f(dy + x_0) \in \mathbb{Z}[y]$ is irreducible.

We can then try to find primes $\ell = f(x_1)$ for some $x_1 \equiv x_0 \mod (-D)$ and test whether $p(x_1)$ is prime as well.

We easily check that if $a(x_1)$, $b'(x_1)$ are constructed as above and $p(x_1)$ is prime, there exists an elliptic curve over the prime field $\mathbb{F}_{p(x_1)}$ with complex multiplication by the maximal order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D})$ such that the Frobenius endomorphism of E corresponds to the element

$$\frac{a(x_1) \pm \frac{b'(x_1)}{d}\sqrt{d}}{2} \in \mathcal{O}.$$

The order $\#E(\mathbb{F}_{p(x_1)})$ is equal to

$$\frac{(a(x_1)-2)^2 - \frac{b'(x_1)^2}{d}}{4}$$

and will by construction be divisible by ℓ.

The degrees of $a(x)$ and $b'(x)$ are less than or equal to $\deg(f) - 1 = d_f - 1$. Hence, for a fixed k the ratio $\frac{\log p}{\log \ell}$ will tend to $2 - 2/d_f$ for $\ell \to \infty$ which is strictly less than 2. In special cases, the relation between ℓ and p will be even better.

Remark 2.1. (1) Note that the assumption that $a(x)$ and $b'(x) \in \mathbb{Z}[x]$ is very strong since only few number fields M have a power integer basis. One possible approach is to replace M by the smallest cyclotomic field containing ζ_n and $\sqrt{d}$ which is usually larger than the compositum of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\zeta_n)$. In any case, the discriminant $|D|$ should not be too large. Experiments show that this idea works well if $|D| \leq 20$.

(2) The integer ℓ does not have to be a prime, but it should be prime up to some small cofactor c, e.g. $c \leq 10$.

3. Special Cases With a Better Relation Between ℓ and p

We demonstrate our idea presenting several examples. The first example has already been considered in [3]. It can easily be deduced from our general approach.

In all our examples, the number field $M = \mathbb{Q}(\sqrt{D}, \zeta_n)$ is a cyclotomic field and therefore has a power integer basis.

(1) Let $k = 9$, $M = \mathbb{Q}(\zeta_9)$ and take $D = -3$. The ninth cyclotomic polynomial is given by $x^6 + x^3 + 1$. Suppose $\ell = x_0^6 + x_0^3 + 1$ for some integer x_0 and let $D = -3$. We would like to construct a suitable Frobenius element $\frac{a+b\sqrt{-3}}{2}$. The element a has to be equal to $\alpha_9 + 1$ where α_9 is a ninth root of unity modulo ℓ. We set $a = x_0 + 1$.
Moreover b should be equal to

$$\frac{\pm(a-2)}{\sqrt{-3}} \equiv \frac{\pm\sqrt{-3}(a-2)}{3} \equiv \frac{(x_0-1)(2x_0^3+1)}{3} \mod \ell.$$

We now choose $x_0 \equiv 1 \mod 3$. Then $a \equiv b \mod 2$ and $p = \mathrm{Norm}_{K/\mathbb{Q}}(\frac{a+b\sqrt{-3}}{2})$ is of size $O(\ell^{\frac{4}{3}})$.
Note that we get a better ratio $\frac{\log p}{\log \ell}$ because the degree of the polynomials $a(x)$ and $b'(x)$ are < 5, i.e. they are smaller than expected.

(2) Let $k = 10$, $M = \mathbb{Q}(\zeta_{10}, \sqrt{-1})$ and $D = -4$. The number field M is generated by the polynomial $x^8 - x^6 + x^4 - x^2 + 1$. The primitive 10th roots of unity are represented by the polynomials

$$x^2, -x^4, -x^6 + x^4 - x^2 + 1, x^6$$

and the roots of -1 are given by the polynomials $\pm x^5$.
Suppose that ℓ is equal to $x_0^8 - x_0^6 + x_0^4 - x_0^2 + 1$ for some integer x_0. Set $a = (-x_0^6 + x_0^4 - x_0^2 + 2)$. Then b should be equal to

$$\frac{\pm(a-2)}{\sqrt{-1}} = \frac{\pm(-x_0^6 + x_0^4 - x_0^2)}{x_0^5} \equiv \pm(-x_0^5 + x_0^3) \mod \ell.$$

We have to ensure that $\mathrm{Norm}_{K/\mathbb{Q}}(\frac{a+b\sqrt{-1}}{2})$ is an integer and is prime.
In this case, p is of order $O(\ell^{\frac{3}{2}})$.

(3) Let q be a prime. Consider $M = \mathbb{Q}(\zeta_q, i)$ and $k = q$. In this case the minimal polynomial is given by

$$f(x) = x^{2q-2} - x^{2q-4} + x^{2q-6} - x^{2q-8} + \cdots + 1.$$

Note that $f(x)(x^2+1) = x^{2q} + 1$. Hence $x^{2q} = -1 \mod f(x)$, i.e. the element $\sqrt{-1}$ corresponds to $\pm x^q \mod f(x)$.
Moreover we have x^2 is a primitive $2q$-th root of unity, i.e. $-x^2$ is a q-th root of unity. We can set $a(x) = -x^2 + 1$ and $b'(x) = (-x^2 - 1)x^q = -x^{q+2} - x^q$. The ratio $\frac{\log(p)}{\log(\ell)}$ is approximately $\frac{q+2}{q-1}$.

(4) Let q be a prime. Consider $M = \mathbb{Q}(\zeta_q, \zeta_3)$ and $k = q$. In this case the minimal polynomial is given by

$$f(x)=\frac{x^{2q}-x^q+1}{x^2-x+1}.$$

We have $f(x)(x^3+1)\Phi_{2q}(x)=x^{3q}+1$ where $\Phi_{2q}(x)$ is the $2q$-th cyclotomic polynomial and $f(x)(x^2-x+1)=x^{2q}-x^q+1$. As above we see that $-x^3$ is a q-th root of unity. We can choose $a(x)=-x^3+1$. Now $(2x^q-1)^2+3=4(x^{2q}-x^q+1)\equiv 0 \mod f(x)$. So $(2x^q-1)$ corresponds to the element $\sqrt{-3}$ and we can set $b'(x)=(-x^3-1)(2x^q+1)$. The ratio $\frac{\log(p)}{\log(\ell)}$ is approximately $\frac{q+3}{q-1}$.

(5) In most cases, $D=-3$ or $D=-4$ give the optimal ratio for $\log p/\log \ell$. But in some rare cases there might be better choices for D.
Let $k=18$ and take $D=-8$. Set $M=\mathbb{Q}(\zeta_{72})$.

The 72nd cylcomotic polynomial is given by $\Phi_{72}(x)=x^{24}-x^{12}+1$. The polynomial x^4 represents a primitive 18th root of unity and $\pm x^{15}\pm x^9\mp x^3$ represent the two roots of $\sqrt{-2}$.

We get $a(x)=x^4+1$ and $b'(x)=-x^{19}+x^{15}-x^{13}+x^9+x^7-x^3$. The polynomial $p(x)=\frac{1}{4}\left(a(x)^2+\frac{1}{2}b'(x)^2\right)$ takes integer values for $x=x_0$ iff x_0 is odd.
Note that our method fails if we use $D=-3$ for $k=18$ and for $D=-4$ the ratio $\log p/\log \ell$ is approximately $11/6$ which is worse than $(38/\varphi(72))=(19/12)$.

Remark 3.1. We implemented an algorithm which takes as input an imaginary quadratic discriminant D, the embedding degree k and an integer n divisible by D and k. It generates the field $M=\mathbb{Q}(\zeta_n)$, computes the polynomials $a(x)$, $b'(x)$ and $p(x)$ as in Section 2. It then tests whether $p(x)$ is irreducible and takes prime values for some x_0.

We started some experiments with different values for D and came up with the following table. We found the following ratios for $\log p/\log \ell$ which are probably optimal.

k	D	$\frac{\log p}{\log \ell}$	k	D	$\frac{\log p}{\log \ell}$
6	$-4,-7$	$\frac{3}{2}$	7	-4	$\frac{3}{2}$
8	-3	$\frac{5}{4}$	9	-3	$\frac{4}{3}$
10	-4	$\frac{3}{2}$	11	-4	$\frac{13}{10}$
12	-3	$\frac{3}{2}$	13	-4	$\frac{5}{4}$
14	-3	$\frac{3}{2}$	15	-3	$\frac{3}{2}$
16	$-3,-4$	$\frac{11}{8}$	17	-4	$\frac{19}{16}$
18	-8	$\frac{19}{12}$	19	-4	$\frac{7}{6}$
20	-3	$\frac{11}{8}$	21	-3	$\frac{4}{3}$

4. Cryptographically Interesting Examples

4.1. Primes with Low Hamming Weight

Since evaluating the pairing can be seen as multiplying a point on the curve by ℓ, pairing based cryptography is very efficient if the prime ℓ has low signed Hamming weight (see [4,9]). For the signed Hamming weight we allow the coefficients of the binary expansion to be $-1, 0, 1$.

Using the method in Section 2, we find some particularly nice examples. To find these examples we run through cyclotomic fields with discriminant divisible by 3 or 4. For each field, we determine the minimal polynomial $f(x)$ and test whether $f(x_0)$ is prime for some x_0 of low Hamming weight, say $x_0 = 2^i$, $x_0 = 2^i \pm 2^k$ or $x_0 = 3^i$. Next we choose a discriminant $D = -3, -4$, compute the corresponding polynomials $a(x)$ and $b'(x)$ and test whether $\frac{a(x_0)^2 - d(b'(x_0)'d)^2}{4}$ (where $d = -1$ resp. -3) is prime, too.

(1) Take $M = \mathbb{Q}(\zeta_{15})$, $k = 15$ and the imaginary quadratic field of discriminant $D = -3$. Let $x_0 = 2^{32} + 1$ and $\ell = \Phi_{15}(x_0)$. The prime ℓ has 257 binary digits and signed Hamming weight 17. Set $a = x_0^4 + 1$ and $b' = 2x_0^7 - 2x_0^6 - 2x_0^5 + x_0^4 - 2x_0^3 + 2x_0^2 - 3$. The prime p is given by $\frac{1}{4}(a^2 + 3(\frac{b'}{3})^2)$. It is of order $O(\ell^{\frac{7}{4}})$.

(2) Take $M = \mathbb{Q}(\zeta_{20})$, $k = 10$ and the imaginary quadratic field of discriminant $D = -4$.
Let $x_0 = 2^{23} + 1$ and $\ell = \Phi_{20}(x_0)$. We have $\lfloor \log_2(\ell) \rfloor \sim 184$ and ℓ has signed Hamming weight 17. Set $a = x_0^2 + 1$ and $b = x_0^7 - x_0^5$. The prime $p = \frac{1}{4}(a^2 + b^2)$ is of order $O(\ell^{\frac{7}{4}})$.

(3) Take $M = \mathbb{Q}(\zeta_{12})$, $k = 12$ and the imaginary quadratic field $D = -3$.
Let $x_0 = 2^{39} + 2^{11} + 2^{10}$ and $\ell = \Phi_{12}(x_0)$. We have $\lfloor \log_2(\ell) \rfloor \sim 157$ and ℓ has signed Hamming weight 21. Set $a = -x_0^3 + x_0 + 1$ and $b' = x_0^3 - 2x_0^2 + x_0 + 1$. The prime p is of order $O(\ell^{\frac{3}{2}})$.

4.2. Primes with Fast Addition Chain

There exist natural numbers whose Hamming weight is not particularly small but which still allow a fast scalar multiplication.

LEMMA 4.1. *Let P be a point on an elliptic curve and let*

$$m = 2^{j_1} \pm 2^{j_2} \pm 2^{j_3}$$

where $0 \le j_3 < j_2 < j_1$. Then mP can be computed with j_1 doublings and two additions/subtractions.

Note that a subtraction has the same complexity as an addition, since taking the inverse on an elliptic curve is a free operation.

Proof. Set $Q_1 = 2^{j_3} P$, $Q_2 = 2^{j_2 - j_3} Q_1$ and $Q_3 = 2^{j_1 - j_2} Q_2$. We need j_1 doublings to compute Q_1, Q_2 and Q_3 and 2 additions/subtractions to compute $Q_3 \pm Q_2 \pm Q_1$. ∎

We can now consider the values of certain cyclotomic polynomials at m given as above.

COROLLARY 4.2. *Let f be a polynomial of degree s with coefficients in $\{0, \pm 1\}$ and t non-zero coefficients. Then $f(m)P$ with m given as in Lemma 4.1 can be evaluated with sj_1 doublings and $2s + t - 1$ additions/subtractions.*

For the proof we just count the number of operations.

EXAMPLE 4.3. (1) Take $m = 2^{22} + 2^{13} + 1$ and consider $M = \mathbb{Q}(\zeta_{24})$ with $k = 8$. We have $\Phi_{24}(x) = x^8 - x^4 + 1$. Set $\ell = \Phi_{24}(m)$. We can calculate ℓP with only $8 \cdot 22 = 176$ doublings and 18 additions. Note that the signed Hamming weight of $\Phi_{24}(m)$ is larger than 30.

We have $\lfloor \log_2(\ell) \rfloor \sim 176$. Set $a = x_0^5 - x_0 + 1$ and $b' = x_0^5 + 2x_0^4 + x_0 - 1$. The prime p is of order $O(\ell^{\frac{5}{4}})$. The corresponding curve defined over $\mathbb{F}_p$ is given by $y^2 = x^3 + 41$.

Alternatively, we can take $m = 2^{23} + 2^{17} + 2^6$. In this case, the evaluation takes $8 \cdot 23 = 184$ doublings and 18 additions. We set $a = -x_0^5 + x_0 + 1$ and $b' = -x_0^5 + 2x_0^4 - x_0 - 1$. The prime is of order $O(\ell^{\frac{5}{4}})$. The elliptic curve over $\mathbb{F}_p$ is given by $y^2 = x^3 + 23$.

Or we take $m = 2^{22} - 2^{10} - 2^4$ and $-x_0^5 + x_0 + 1$ and $b' = -x_0^5 + 2x_0^4 - x_0 - 1$. In all three cases, we find an elliptic curve over $\mathbb{F}_p$ with $p = \frac{1}{4}\left(a^2 + 3(\frac{b}{3})^2\right)$ with complex multiplication by $\mathbb{Z}[\zeta_3]$. The corresponding elliptic curve is given by $y^2 = x^3 + 32$.

(2) Take $\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$ and $m = 2^{20} + 2^{14} + 4$. Then $\ell = \Phi_{20}(m)$ can be computed using 160 doublings and 20 additions.

Let $k = 10$ and set $a = -x_0^6 + x_0^4 - x_0^2 + 2$ and $b = x_0^5 - x_0^3$. We find an elliptic curve with complex multiplication by $\mathbb{Z}[i]$ over $\mathbb{F}_p$ with $p = \frac{1}{4}(a^2 + b^2)$ of order $O(\ell^{\frac{3}{2}})$. The equation of the elliptic curve is $y^2 = x^3 + x$.

Acknowledgments

The authors thank S. Galbraith and M. Scott for helpful comments on the paper. Especially, S. Galbraith suggested to look for examples where ℓ has small Hamming weight.

The necessary computations for the examples in Sections 3 and 4 were done using Magma (http://magma.maths.usyd.edu.au/magma/).

References

1. A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, Vol. 61 (1993), pp. 29–68.
2. R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, Vol. 11, No. 2 (1998), pp. 141–145.
3. P. Barreto, B. Lynn and M. Scott, Constructing elliptic curves with prescribed embedding degrees. *Proceedings of the Third Workshop on Security in Communication Networks (SCN'2002), LNCS*, 2576, 2003.
4. P. S. L. M. Barreto, H. Y. Kim, B. Lynn and P. Scott, Efficient algorithms for pairing based cryptosystems. *Crypto 2002, LNCS*, 2442 (2002), pp. 354–368.
5. D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing. *Asiacrypt '01, LNCS*, 2248 (2001), pp. 514–532.
6. R. Dupont, A. Enge, and F. Morain, Building curves with arbitrary small MOV degree over finite fields. to appear in *Journal of Cryptography*, 2002.
7. M. Franklin and D. Boneh, Identity-based encryption from the Weil pairing. *Proceedings Crypto '01, LNCS*, 2139 (2001), pp. 213–229.
8. G. Frey, M. Müller and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Transactions on Information Theory*, Vol. 45 No. 5 (1999), pp. 1717–1718.
9. S. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing. *ANTS IV, LNCS*, 2369 (2002), pp. 324–337.
10. A. Joux, A one round protocol for tripartite Diffie-Hellman. *Proceedings of ANTS, LNCS* 1838 (2000), pp. 385–393.
11. A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, Vol. 39, No. 5 (1993), pp. 1639–1646.
12. E. Verheul, Self-blindable credential certificates from the Weil pairing. *Advances in Cryptology – Asiacrypt 2001, LNCS*, 2248 (2002), 533–551.