J. Cryptology (2005) 18: 79–89
DOI: 10.1007/s00145-004-0219-7

Journal of
CRYPTOLOGY

Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields*

Régis Dupont, Andreas Enge, and François Morain
Laboratoire d'Informatique de l'École polytechnique (LIX),
CNRS/UMR 7650, INRIA-Futurs,
F-91128 Palaiseau Cedex, France
{dupont,enge,morain}@lix.polytechnique.fr

Communicated by Dan Boneh

Received 18 July 2002 and revised 8 October 2003
Online publication 21 October 2004

Abstract. We present a fast algorithm for building ordinary elliptic curves over finite prime fields having arbitrary small MOV degree. The elliptic curves are obtained using complex multiplication by any desired discriminant.

Key words. Elliptic curves over finite fields, MOV degree, Complex multiplication.

1. Introduction

Beginning with the independent works of Sakai et al. [30] and Joux [23], the Weil and Tate pairings on elliptic curves have recently found numerous applications in the design of cryptosystems, such as identity-based encryption [4], short signatures [5], identity-based signatures [8], [22], [29], [30], non-interactive key distribution [12], [30] and authenticated key agreement [34].

In order to implement such protocols, one needs curves over which the Weil or Tate pairings can be efficiently computed, i.e. curves with a sufficiently small MOV degree. Supersingular curves have received particular attention in this context since it has been proved [25] that their MOV degree k is always less than or equal to 6. However, the security of pairing-based protocols depends on the hardness of the discrete logarithm problem in an extension of degree k of the base field of the curve. Thus, k must not be *too* small, and it is of interest to generate ordinary elliptic curves with a k of moderate size, but which is not restricted to $\{1, 2, 3, 4, 6\}$ (in [5] Boneh et al. leave it as an open problem to build curves with $k = 10$).

* The third author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

In [27] Miyaji et al. give explicit conditions to obtain ordinary curves with specified k. Their method leads to solving a Diophantine equation whose genus increases with the value of Euler's totient function $\varphi(k)$. They treat the case where $\varphi(k) = 2$ (that is $k = 3$, 4 and 6) by showing that the Diophantine equation reduces to Pell's equation.

Recently Barreto et al. [3] proposed two methods of construction. Their curves have complex multiplication by a prescribed quadratic order of discriminant $-D$. The first method is for $D = 3$ only, and k of the form $3^i 2^j k'$, k' a prime greater than 3. The curves they obtain have a subgroup of large prime order ℓ. If k is very large, then the ratio of $\log p/\log \ell$ is close to 1. The second method is more general and works for any D. It can be shown that the ratio $\log p/\log \ell$ for the produced curves is close to 2.

We present an alternative method for achieving the same goal, but using a different parameterisation of (p, ℓ). Our idea is to use *maximal curves* built via complex multiplication. Our curves also suffer from the fact that the ratio $\log p/\log \ell$ is usually 2. Since their security will depend on ℓ and not on the cardinality of the curve, the use of such curves in existing protocols will often result in an increase in the size of the ciphertexts or signatures generated.

Section 2 contains classical facts on complex multiplication. In Section 3 we present our approach, and we provide numerical examples in Section 4.

2. Building an Elliptic Curve with Given Cardinality

We briefly summarise the relevant elements of complex multiplication needed for our purpose. References are [10] and [33]; [1] and [24] provide a more computational perspective.

Suppose we want to build an elliptic curve $E/\mathbb{F}_q$ having $q + 1 - t$ points, for given q and t satisfying the Hasse bound $|t| \leq 2\sqrt{q}$. If we write $\Delta = t^2 - 4q = -g^2 D$, where $-D$ is a fundamental quadratic discriminant, then the curve E can be obtained as a curve having complex multiplication by $-D$. The construction, as described for instance in [1] and [15], has a time complexity depending on the class number $h(-D)$, which grows as $D^{1/2+o(1)}$ by Siegel's theorem [32].

To our knowledge, the currently best algorithms, using the constructions of [1], [15], and [13], can handle class numbers of up to a few thousands (our implementation computes a curve with associated class number $h(-D) = 5000$ in about 40 min on a Pentium III clocked at 800 MHz).

Keeping the class number $h(-D)$ of manageable size amounts to keeping D relatively small, and this imposes serious restrictions on the choice of q and t. One possible approach, which we adopt here, is directly to force $\Delta = t^2 - 4q$ to be of small absolute value. To obtain Δ of reasonable size, we need $|t| = \lfloor 2\sqrt{q} \rfloor$. To see why, write $|t| = 2\sqrt{q} - u$ to obtain

$$t^2 - 4q = -4u\sqrt{q} + u^2.$$

As already observed in [28], for $u \geq 1$ the class number associated to $t^2 - 4q$ then grows as $O(q^{1/4})$.

The only possible alternative to having $|t| = \lfloor 2\sqrt{q} \rfloor$ is to force Δ to have a large square factor, so that D may be small even if $|\Delta|$ is large. Barreto et al. have suggested

such an approach in [3]. Their technique leads to rather small values of t, so that they end up with curves close to the centre of the Hasse interval instead of on its border.

3. Curves with Small MOV Degree

3.1. *The Problem*

Let $E/\mathbb{F}_q$ have cardinality m and let ℓ be a prime factor of m such that $\ell \nmid q-1$. The MOV degree of $E/\mathbb{F}_q$ relative to ℓ is defined to be the smallest integer k such that $\ell \mid q^k - 1$, i.e. it is the order of q in the group $\mathbb{F}_\ell^\times$. A theorem by Balasubramanian and Koblitz [2] then states that $E/\mathbb{F}_{q^k}$ contains ℓ^2 points of ℓ-torsion, which implies that the Weil pairing e_ℓ is defined on the following groups:

$$e_\ell\colon\ E/\mathbb{F}_{q^k}[\ell] \times E/\mathbb{F}_{q^k}[\ell] \to \mathbb{F}_{q^k}^\times.$$

Alternatively, the computationally preferable Tate pairing can be defined on the same groups.

For cryptographic applications, the prime ℓ should be large (typically the largest factor of m), and from now on we omit ℓ when talking about MOV degrees. For the pairing to be efficiently computable, the MOV degree k should be relatively small since the algorithm used to compute pairings, due to Miller [26], runs in time $O(M(q^k)\log \ell)$, where $M(q^k)$ is the time needed for a multiplication in $\mathbb{F}_{q^k}$.

Now since k is the order of q modulo ℓ it must divide $\ell - 1$, and in this case, the probability of q having order k should heuristically be proportional to $k/(\ell-1)$. This means that for a random curve, k is unlikely to be small, and we have to force it in some way.

Writing $m = q + 1 - t$, the problem we have to solve is the following: find integers (ℓ, q, t) such that ℓ is prime, q is a power of a prime, $\ell \mid q + 1 - t$ and q is of order k modulo ℓ.

3.2. *Our Solution*

We suppose k is fixed and explain how we can achieve examples of curves having this value of k as MOV degree.

Any prime power q can be written uniquely as

$$q = n^2 + a \qquad \text{with} \quad n \geq 1 \quad \text{and} \quad 0 \leq a \leq n$$

or

$$q = n^2 + n + a \qquad \text{with} \quad n \geq 1 \quad \text{and} \quad 1 \leq a \leq n.$$

As discussed in Section 2, we build curves via the CM method with $|t| = \lfloor 2\sqrt{q} \rfloor$, that is,

$$t = \pm 2n \qquad \text{for} \quad q = n^2 + a$$

and

$$t = \pm(2n+1) \qquad \text{for} \quad q = n^2 + n + a,$$

respectively.

To simplify the exposition, we assume for the time being that $q = n^2 + a$ and $t = +2n$, and come back to the other cases further below. Then $m = q + 1 - t = (n-1)^2 + a$, which should be divisible by the unknown ℓ. Thus, the order of q modulo ℓ being k is equivalent to

$$\Phi_k(t-1) \equiv 0 \bmod \ell,$$

where Φ_k is the kth cyclotomic polynomial, and $k \mid \ell - 1$. (This last condition ensures that the order of q is indeed k and not a proper divisor of k. Indeed, it implies that there are $\varphi(k)$ elements of order k modulo ℓ, which must be given by the roots of Φ_k. In practice, the condition will usually be fulfilled automatically, see the examples of Section 4.)

Combining these equations, we see that n, a and ℓ are related by

$$\begin{cases} \Phi_k(2n-1) \equiv 0 \bmod \ell, \\ (n-1)^2 + a \equiv 0 \bmod \ell. \end{cases} \tag{1}$$

Conversely, any natural numbers n, a and ℓ satisfying this system and such that ℓ is prime, $q = n^2 + a$ is a prime power and $k \mid \ell - 1$ lead to a solution of our problem.

To eliminate one of the three unknowns, we consider the polynomials $P_k(X) = \Phi_k(2X-1)$ and $Q(X, a) = (X-1)^2 + a$ and their resultant

$$R_k(a) = \operatorname{Res}_X(P_k(X), Q(X, a)).$$

The first few values of $R_k(a)$ are given in Table 1.

Proposition 3.1. *$R_k(X) \in \mathbb{Z}[X]$ is irreducible. Its leading term is $4^{\varphi(k)}X^{\varphi(k)}$. Its constant coefficient is p^2 if k is a power of the prime p and 1 otherwise. The content of R_k is 1, unless k is a power of 2, in which case the content is 4.*

Proof. Suppose that $k > 2$, since for $k = 2$ the assertion is trivial. Writing the resultant of a polynomial f with leading coefficient c and a polynomial g as $c^{\deg g} \prod_{\alpha \text{ root of } f} g(\alpha)$ (see for instance [18]), we obtain

$$R_k(X) = (2^{\varphi(k)})^2 \prod \left(X + \left(\frac{\zeta^i - 1}{2} \right)^2 \right),$$

Table 1. Values of the resultant R_k.

k	$R_k(a)$
2	$4a + 4$
3	$16a^2 + 12a + 9$
4	$16a^2 + 4$
5	$256a^4 + 320a^3 + 160a^2 + 25$
6	$16a^2 - 4a + 1$
7	$4096a^6 + 7168a^5 + 5376a^4 + 2240a^3 + 784a^2 - 196a + 49$
8	$256a^4 + 256a^3 + 128a^2 - 32a + 4$
9	$4096a^6 + 6144a^5 + 2304a^4 + 192a^3 + 576a^2 - 108a + 9$
10	$256a^4 + 64a^3 + 96a^2 - 16a + 1$
11	$1048576a^{10} + 2883584a^9 + 3604480a^8 + 2703360a^7 +$ $1351680a^6 + 473088a^5 + 123904a^4 + 17424a^2 - 2420a + 121$

where ζ is a primitive kth root of unity and the product is taken over the integers $i \in \{1, \ldots, k-1\}$ coprime to k. In particular, R_k is of degree $\varphi(k)$, and all of its coefficients, except possibly for the constant one, are divisible by 4. Furthermore, its constant coefficient is the square of the norm of $\zeta - 1$, which equals 1 or p (see [11]) according to the condition given in the proposition.

Let $\alpha = ((\zeta - 1)/2)^2$ be a root of $R_k(X)$. Then either α still generates $\mathbb{Q}(\zeta)/\mathbb{Q}$, in which case R_k is irreducible, or $\mathbb{Q}(\alpha)$ is a subfield of index 2 of $\mathbb{Q}(\zeta)$. In the latter case, α is of degree $\varphi(k)/2$ over $\mathbb{Q}$, whence there exists a monic polynomial $P \in \mathbb{Q}[X]$ of degree $\varphi(k)/2$ such that $P(4\alpha) = P(((\zeta - 1)^2) = 0$. Since $P((X-1)^2)$ is monic and of degree $\varphi(k)$, it follows that

$$\Phi_k(X) = P((X-1)^2).$$

However, the coefficient of $X^{\varphi(k)-1}$ of $P((X-1)^2)$ is $-\varphi(k)$, while the same coefficient of Φ_k is the negative sum of $\varphi(k)$ roots of unity different from 1 and -1 for $k > 2$, a contradiction. □

To obtain a solution to (1), we now fix values of a. Notice that this leads to $\Delta = t^2 - 4q = -4a = -g^2 D$ with some fundamental discriminant $-D$, and a must be chosen such that D is not too large. We try to factor $R_k(a)$ and to obtain sufficiently large prime factors ℓ. If we succeed, we compute $\gcd(P_k(X), Q(X, a)) \bmod \ell$ to get n. Then we test whether $n^2 + a$ is a prime (obtaining a non-trivial prime power seems hopeless), in which case we build the CM curve over $\mathbb{F}_q$ having complex multiplication by the fundamental discriminant $-D$.

The other possible choices for q and the sign of t lead to the following systems:

$$\begin{cases} \Phi_k(-2n-1) \equiv 0 \bmod \ell, \\ (n+1)^2 + a \equiv 0 \bmod \ell, \\ t = -2n, \\ q = n^2 + a, \\ \Delta = -4a. \end{cases} \tag{2}$$

$$\begin{cases} \Phi_k(2n) \equiv 0 \bmod \ell, \\ n(n-1) + a \equiv 0 \bmod \ell, \\ t = +(2n+1), \\ q = n^2 + n + a, \\ \Delta = -4a + 1. \end{cases} \tag{3}$$

$$\begin{cases} \Phi_k(-2n-2) \equiv 0 \bmod \ell, \\ (n+1)(n+2) + a \equiv 0 \bmod \ell, \\ t = -(2n+1), \\ q = n^2 + n + a, \\ \Delta = -4a + 1. \end{cases} \tag{4}$$

The corresponding resultants have the same properties as found for R_k in Proposition 3.1, and the algorithm is completely analogous.

3.3. *Algorithm*

Our procedure takes as input k and a security parameter L, corresponding to the minimal size of an elliptic curve subgroup for which the discrete logarithm problem is computationally intractable. Further input is a list $\mathcal{D}$ of absolute values of suitable discriminants. This list could simply consist of all small quadratic discriminants, or additional constraints such as a lower bound for the class number (see [17]) or a smoothness property of the class number (see [21] and [14]) could be taken into account. It is also possible to fix the discriminant completely. Again, we formulate the algorithm for the case $q = n^2 + a$ and $t = +2n$ only; the other three cases are obtained in a straightforward manner.

procedure SMALLK(k, L, $\mathcal{D}$)
for $D \in \mathcal{D}$ **do**
  for $g := g_{\min} \cdots g_{\max}$ such that $4 \mid g^2 D$ **do**
  1. let $a := g^2 D/4$;
  2. factor $R_k(a)$;
  3. **if** $R_k(a)$ has a prime factor $\ell \geq L$ such that $k \mid \ell - 1$ **then**
     3.1 compute a root n of $\gcd(P_k(X), Q(X, a)) \bmod \ell$;
     3.2 **for** $s := 0 \cdots s_{\max}$ **do**
         if $a \leq n + s\ell$ **then**
           – let $p := (n + s\ell)^2 + a$;
           – **if** p is prime **then** compute E;

Compared with the straightforward algorithm based on the observations of Section 3.2, the procedure above contains two refinements:

- We generally do not start at $g = 1$; as a matter of fact, since $R_k(a) \sim (4a)^{\varphi(k)} = (g^2 D)^{\varphi(k)}$ and R_k is increasing, we first compute the minimal $g_{\min}$ such that $R_k(a) \geq L$. In order to keep $R_k(a)$ close to L, it may be necessary to impose an upper bound $g_{\max}$.
- Any number congruent to n modulo ℓ may be used in its place. This is why we replace n in Step 3.2 by $n + s\ell$ for small values of s to obtain a higher yield of suitable elliptic curves. Notice that in general, n will be of the order of ℓ for $s = 0$, so that the bitsize of p is about twice that of ℓ. For other values of s, the field order p will be larger by about $2\log_2(s + 1)$ bits, which is negligible for small values of s. Moreover, in situations with a low density of suitable elliptic curves, the higher yield induced by having $s_{\max} > 0$ may lead to an overall smaller value of p, see the example for $k = 50$ in Section 4.

  If s is set to negative values, then the curve trace t will be on the opposite border of the Hasse interval. Thus, it is possible to treat the two cases of positive and negative trace at the same time.

Notice, by the way, that we do not make use of the fact that ℓ is prime in Step 3.1. Indeed, the algorithm can be used to obtain curves of given MOV degree also for composite ℓ.

3.4. *Heuristics*

Let us sketch a rough analysis of our algorithm. We consider the situation where we expect $R_k(a)$ to be "as prime as possible", that is, we look for values $R_k(a)$ that are

prime or, if k is a power of 2, four times a prime; the cofactor 4 in the latter case cannot be avoided according to Proposition 3.1. Heuristically, we assume that the values of the polynomial R_k behave as random numbers of the same size. Then, if D and g are chosen in a range where the values of R_k are around L, the probability of obtaining an (almost) prime value is proportional to $1/\log L$. The integer n has a bit length of about $2\log_2 L$, and the chances of p being prime are proportional to $1/\log L$, too. This means that we should find suitable elliptic curves after $O(\log^2 L)$ trials.

4. Numerical Examples

To demonstrate our ideas, we have implemented the search for suitable CM parameters of elliptic curves in MAGMA [9]. The corresponding CM curves $Y^2 = X^3 + AX + B$ were then constructed with our own C++ program relying on GMP [19], MPFR [20], MPC [16] and NTL [31]. If A is required to be of a special form (e.g. $A = -3$), this may be achieved via isomorphisms or isogenies as explained in [7]. For each curve, we provide the corresponding class number h, as well as the running time r for the curve construction in seconds, measured on a Pentium 4 running at 1.8 GHz.

Factoring $R_k(a)$ in Step 2 of the algorithm could be done with a large sieve, reminiscent of the NFS algorithm. In practice, we content ourselves with using a bound B and trial division to find values of $R_k(a)$ which are composed of small primes below B and a large prime cofactor. In our experiments, we chose $B = 10^4$.

We first provide a few examples for small prime values of k. For such small cases, it is not necessary to loop over D and g; instead, we may directly loop over a, as the resulting discriminants will be sufficiently small. Also, we may put $s_{\max} = 0$. We chose $L = 10^{18}$. Running the algorithm for $p = n^2 + a$ and $t = +2n$ for the first 10,000 possible values of a, starting with the minimal value $a = 7906$, yields ten suitable parameter combinations in 13 s. The first curve (for $k = 5$) is given by

$$\begin{aligned} a &= 7984, \\ D &= 499, \\ h &= 3, \\ p &= 916000224356688812977608191082736 09, \\ \ell &= 1040375393410195481, \\ A &= 17400269694421412435880788357515251, \\ B &= 81201258573966591367443679001737838, \\ r &= 0.1 \text{ s}. \end{aligned}$$

For $k = 7$ and looking for curves with $p = n^2 + a$ and $t = -2n$, the first 10,000 values of a yield 33 suitable parameter combinations in 21 s. The last resulting curve is given by

$$\begin{aligned} a &= 10066, \\ D &= 40264, \\ h &= 72, \end{aligned}$$

$$
\begin{aligned}
p &= 68232381434104442417727981407880784676003947,\\
\ell &= 13532331455189147830139,\\
A &= 120577074038821139781947136942850150153507 90,\\
B &= 30782598747289556791372469598816938235568509,\\
A &= -3,\\
B &= 62625802927525881688245544206408777151296438,\\
r &= 0.6\text{ s}.
\end{aligned}
$$

In the following, we provide examples of cryptographic size parameters. We choose $L = 2^{200}$. For $k = 10$, this yields a minimal value for a of 281474976710700. This is by far too large to serve as a complex multiplication discriminant. Instead, we fix a discriminant $-D$, say as the first discriminant of class number $h = 4096$, $D = 4599839$, and loop over g in the range from $g_{\min} = 15646$ to $g_{\max} = g_{\min} + 100000$ to find curves of the form $p = n^2 + a$ and $t = +2n$. As before, we put $s_{\max} = 0$. This yields three curves after 190 s, the first of which is computed as follows:

$$
\begin{aligned}
a &= 2851946178390000 = 24900^2 \cdot 4599839,\\
D &= 4599839,\\
h &= 4096,\\
p &= 26583877300690675075645839413139198533414446909174\backslash\\
&\quad 08606124019858001080573263503000190636119494020100\backslash\\
&\quad 3625757271755408084936 9 \text{ (407 bits)},\\
\ell &= 25621456065075422729511299019214902729542591998892\backslash\\
&\quad 393498858941 \text{ (204 bits)},\\
A &= 11200689934606448746623138995223367963405096267317\backslash\\
&\quad 28974086005718562911005540411220873407758621459544\backslash\\
&\quad 8038064939327807054430 8,\\
B &= 23867609517085989149655010588871027980606985661378\backslash\\
&\quad 66582586490287914389875058399524997485380753096941\backslash\\
&\quad 4018710731376941443485,\\
r &= 376\text{ s}.
\end{aligned}
$$

The small yield of the algorithm in this case is an indication that it will be beneficial to vary our remaining degree of freedom, the value of $s_{\max}$. Indeed, allowing s to take values up to 10, we find for the same discriminant and the same range of g in about the same computing time altogether 23 parameter combinations for $s_{\max} = 5$ (resp. 52 combinations for $s_{\max} = 10$).

For $\varphi(k)$ large, it may become impossible to keep ℓ close to L. For instance, if $4^{\varphi(k)} \gg L$, then all possible values of a will yield huge values of $R_k(a)$, for which finding prime factors of size L will be very difficult. For the same reason, one should not fix a too large discriminant. However, the phenomenon does not occur even for medium values of k that are beyond the practical range if the discriminant is not chosen too large.

We provide as an example the case $k = 50$, where again we loop over the first 10,000 possible values of a. We let $L = 2^{200}$, $s_{\max} = 0$ and look for curves of the form $p = n^2 + n + a$, $t = +2n + 1$. Then we find six parameter combinations in about 67 s. The one with the smallest value of p is obtained for $a = 697$; it has p of 457 bits and ℓ of 229 bits. So while p is still about twice as large as ℓ, we lose more than a factor of 2 with respect to our target L of 200 bits. Again, we may make use of the additional degree of freedom and let $s_{\max} = 10$. In 88 s this yields 29 suitable parameter combinations, the first of which (for $a = 381$) has p of 410 bits, ℓ of 202 bits and $s = 9$. So while we lose in the ratio $\log p/\log \ell$, which becomes a bit larger than 2, we obtain an absolutely smaller value of p while keeping our elliptic curve security at the level of 200 bits. Another possible approach of improving the yield of the algorithm, namely increasing the trial division bound B, does not turn out to be very successful. With $s_{\max} = 10$ as before, but $B = 10^6$ instead of $B = 10^4$, the number of curves found certainly becomes larger and reaches 43. However, the running time also increases, and very much, to 2200 s.

5. Conclusions

We have described a method yielding elliptic curves E defined over a prime field $\mathbb{F}_p$ having a given MOV degree k. Our curves have subgroups of prime order ℓ, of size $O(\sqrt{p})$. Roughly speaking, a secure $\ell = 2^{200}$ implies a field of size 2^{400}. Note that we implicitly assume that our way of constructing E is not dangerous, hoping that CM curves are not weak and that solving the discrete logarithm problem in an elliptic curve subgroup of size ℓ within a group of size ℓ^2 is not easier than in an elliptic curve group of size ℓ.

In any case, we doubt that the general problem of constructing elliptic curves over a fixed field $\mathbb{F}_p$ and of fixed prime group order m can be solved.

Acknowledgements

We are grateful to Paulo Barreto and Michael Scott for their helpful remarks, and we thank Pierrick Gaudry for valuable discussions concerning this work. Thanks also to Antoine Joux for suggesting finding examples for large values of k.

Note Added in Proof. Recently, F. Brezing and A. Weng [6] have proposed a new method for solving the problem.

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[2] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *J. Cryptology*, 11:141–145, 1998.

[3] P. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In S. Cimato, C. Galdi, and G. Persiano, editors, *Security in Communication Networks—Third International*

Conference, *SCN* 2002, *Amalfi*, *Italy*, *September* 2002, volume 2576 of Lecture Notes in Computer Science, pages 257–267. Springer-Verlag, Berlin, 2003.

[4] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO* 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, Berlin, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, editor, *Advances in Cryptology – ASIACRYPT* 2001, volume 2248 of Lecture Notes in Computer Science, pages 514–532. Springer-Verlag, Berlin, 2001.

[6] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Available as `http://eprint.iacr.org/2003/143/`, July 2003.

[7] E. Brier and M. Joye. Fast point multiplication on elliptic curves through isogenies. In M. Fossorier, T. Høholdt, and A. Poli, editors, *Applied Algebra*, *Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of Lecture Notes in Computer Science, pages 43–50. Springer-Verlag, Berlin, 2003. (15th International Symposium, AAECC-15, Toulouse, France, May 2003, Proceedings.)

[8] J. Cha and J. Cheon. An identity-based signature from gap Diffie–Hellman groups. In Y. Desmedt, editor, *Public Key Cryptography — PKC* 2003, volume 2567 of Lecture Notes in Computer Science, pages 18–30. Springer-Verlag, Berlin, 2002.

[9] Computational Algebra Group of the University of Sydney. MAGMA, version 2.10, 2003. `http://magma.maths.usyd.edu.au/magma/`.

[10] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. Wiley, New York, 1989.

[11] H. Davenport. *Multiplicative Number Theory*, 2nd edition, volume 74 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1980.

[12] R. Dupont and A. Enge. Provably secure non-interactive key distribution based on pairings. In D. Augot, P. Charpin, and G. Kabatianski, editors, *WCC* 2003 *— Proceedings of the International Workshop on Coding and Cryptography*, pages 165–174. École Supérieure et d'Application des Transmissions, 2003. To appear also in *Discrete Appl. Math*.

[13] A. Enge and F. Morain. Further investigations of the generalised Weber functions. In preparation, 2001.

[14] A. Enge and F. Morain. Fast decomposition of polynomials with known Galois group. In M. Fossorier, T. Høholdt, and A. Poli, editors, *Applied Algebra*, *Algebraic Algorithms and Error-Correcting Codes — AAECC*-15, volume 2643 of Lecture Notes in Computer Science, pages 254–264. Springer-Verlag, Berlin, 2003.

[15] A. Enge and R. Schertz. Constructing elliptic curves from modular curves of positive genus. Submitted, 2001.

[16] A. Enge and P. Zimmermann. MPC—Multiprecision complex arithmetic library, version 0.4.1, 2002. Available at `http://www.loria.fr/~zimmerma/free/`.

[17] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In D. Jungnickel and H. Niederreiter, editors, *Finite Fields and Applications — Proceedings of the Fifth International Conference on Finite Fields and Applications F_q*5, *held at the University of Augsburg*, *Germany*, *August* 2–6, 1999, pages 128–161. Springer-Verlag, Berlin, 2001.

[18] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.

[19] T. Granlund and K. Ryde. GMP—GNU multiprecision library, version 4.1.2, 2002. Available at `http://www.swox.com/gmp/`.

[20] G. Hanrot, V. Lefèvre, K. Ryde, and P. Zimmermann. MPFR—Multiprecision floating point library with exact rounding, version contained in [19], 2002. Available at `http://www.mpfr.org/`.

[21] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In B. Mourrain, editor, *ISSAC* 2001 *— Proceedings of the* 2001 *International Symposium on Symbolic and Algebraic Computation*, pages 175–182. Association for Computing Machinery, New York, 2001.

[22] F. Hess. Efficient identity based signature schemes based on pairings. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography — SAC* 2002, volume 2595 of Lecture Notes in Computer Science, pages 310–324. Springer-Verlag, Berlin, 2003.

[23] A. Joux. A one round protocol for tripartite Diffie–Hellman. In W. Bosma, editor, *Algorithmic Number Theory*, volume 1838 of Lecture Notes in Computer Science, pages 385–393. Springer-Verlag, Berlin, 2000.

[24] G.-J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of Lecture Notes in Computer Science, pages 250–263. Springer-Verlag, Berlin, 1994.
[25] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, IT-39(5):1639–1646, September 1993.
[26] V. Miller. Short programs for functions on curves. Draft, 1986.
[27] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, E84-A(5):1234–1243, May 2001.
[28] F. Morain. Building cyclic elliptic curves modulo large primes. In D. Davies, editor, *Advances in Cryptology – EUROCRYPT* '91, volume 547 of Lecture Notes in Computer Science, pages 328–336. Springer-Verlag, Berlin, 1991.
[29] K. Paterson. Information theory—ID-based signatures from pairings on elliptic curves. *Electron. Lett.*, 38(18):1025–1026, 2002.
[30] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. Presented at SCIS 2000, The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26–28.
[31] V. Shoup. NTL—Number Theory Library, version 5.3, 2002. Available at `http://shoup.net/ntl/`.
[32] C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86, 1935.
[33] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.
[34] N. Smart. Information theory—identity-based authenticated key agreement protocol based on Weil pairing. *Electron. Lett.*, 38(13):630–631, 2002.