Building curves with arbitrary small MOV degree over finite prime fields

R. Dupont, A. Enge, F. Morain*

{dupont, enge, morain}@lix.polytechnique.fr

July 18, 2002

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.

Keywords: elliptic curves over finite fields, MOV degree, complex multiplication.

1 Introduction

Beginning with the independent works of Sakai, Ohgishi and Kasahara [26] and Joux [18], 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 [6, 17, 24, 26], non-interactive key distribution [10, 26] or authenticated key agreement [29].

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 are particularly well suited since it has been proved [20] that their MOV degree is always less than or equal to 6. However, the security of these protocols is directly linked to the MOV degree k, since it assumes that the discrete logarithm problem is hard

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

in an extension of degree k of the base field of the curve. It is thus of interest to be able to generate ordinary elliptic curves with a small MOV degree k, not restricted to $\{1, 2, 3, 4, 6\}$ (in [5], Boneh, Lynn and Shacham leave it as an open problem to build curves with $k = 10$).

In [22] Miyaji, Nakabayashi and Takano 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 $\varphi(k)$. 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, Lynn and Scott [3] proposed an algorithm for building curves over prime finite fields with any k, using complex multiplication by a prescribed quadratic order. The curves they obtain have a subgroup of large prime order ℓ, for which the ratio $\log p/\log \ell$ can be up to 2.

We present an alternative method achieving the same goal, but using a different parametrization of (p, ℓ). Our idea is to use *maximal curves* built via complex multiplication. Our curves also suffer from the fact that the ratio $\log p/\log \ell$ can be up to 2. Since their security will depend on ℓ and not on the cardinality m 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 Brief review of complex multiplication

2.1 Theory

We summarise the relevant elements of complex multiplication needed for our purpose. References are [8, 28] and [1] for more computations.

Let $q = p^d$ be a prime power. An elliptic curve E over $\mathbb{F}_q$ has $m = q + 1 - t$ points where t is an integer such that $|t| \leq 2\sqrt{q}$. Conversely, given an integer t prime[1] to p satisfying the bound, there exists a curve $E/\mathbb{F}_q$ having cardinality $q + 1 - t$. The only known method for building such a curve is to use complex multiplication. Precisely, let $\Delta = t^2 - 4q < 0$ be the discriminant of the order $\mathcal{O}$ generated by the Frobenius of E. Write $\Delta = -f^2 D$, where $-D$ is the discriminant of the imaginary quadratic field

[1] Only a restricted list of t divisible by p can occur, and these lead to supersingular curves that do not interest us in this article.

containing $\mathcal{O}$. Then E can be built as a curve having complex multiplication by the principal order $\mathbb{Z}[(D+\sqrt{-D})/2]$.

Explicit equations for E are derived using the theory of class fields and singular invariants. The algorithms usually proceed in three steps [1, 19, 12]. In the first step, a class polynomial is constructed. This is an irreducible polynomial in $\mathbb{Z}[X]$ of degree h, the class number of $-D$, whose roots generate the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$. By standard arguments of algebraic number theory, h is of size $D^{1/2+o(1)}$. Using the class polynomials described in [11, 12], a class number of a few thousand is tractable. On a Pentium III at 800 MHz, our current implementation computes class polynomials of degree 1000 in about 20 s, for a degree of 5000 it needs about 40 min. In the second step, a root of the class polynomial in $\mathbb{F}_q$ is sought, and this has in fact become the dominant part of the algorithm already for primes of a few hundred bits. Finally, the elliptic curve equation is deduced from the root, which has a negligible cost compared to the previous two steps.

2.2 Building a curve with given cardinality

Suppose we want to build $E/\mathbb{F}_q$ having $q+1-t$ points for given q and t. If t^2 is very small compared to q, then $|\Delta| = Df^2$ is close to $4q$. On average, f will be small and $h(\Delta)$ will be close to $\sqrt{q}$ which makes the whole computation infeasible. (Note that solving this problem would imply being able to do primality proving very fast, for instance yielding small certificates of primality *à la* Pomerance [25].)

To circumvent the problem, one has to devise clever methods, finding parametrisations of (q,t). One of these methods is presented in [3]. Our approach is different and uses the fact that if t^2 is close to $4q$, then $|\Delta|$ and thus D may be small and the method outlined in 2.1 may work. In fact, we need $|t| = \lfloor 2\sqrt{q} \rfloor$. To see why, write $|t| = 2\sqrt{q} - u$ to obtain

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

If $u \geq 1$, then the class number associated to Δ is in $O(q^{1/4})$ (this was already remarked in [23]). Unless we can force Δ to have a large square factor, so that D is small nevertheless, we cannot do anything in this case.

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 $E/\mathbb{F}_q$ relatively 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:

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

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 will 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 [21], runs in time $O(M(q^k)\ell \log \ell)$, 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 k is unlikely to be small, and we have to force it in some ways.

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 come up with examples of curves having this value of k as MOV degree.

Any prime power q can be written uniquely as

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

or

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

As discussed in Section 2.2, we will build curves via the CM method with $|t| = \lfloor 2\sqrt{q} \rfloor$, that is,

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

and

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

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 k-th cyclotomic polynomial. 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 sytem and such that ℓ is prime and $q = n^2 + a$ is a prime power 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

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

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 [15]), we obtain $R_k(X) = \left(2^{\varphi(k)}\right)^2 \prod \left(X + \left(\frac{\zeta^i - 1}{2}\right)^2\right)$, where ζ is a primitive k-th 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 [9]) according to the condition given in the proposition.

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	$1048576a^{10}+2883584a^9+3604480a^8+2703360a^7$
	$+1351680a^6+473088a^5+123904a^4+17424a^2-2420a+121$

Table 1: Values of the resultant R_k

Let $\alpha = \left(\frac{\zeta-1}{2}\right)^2$ 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 $P(4\alpha) = P\left((\zeta-1)^2\right) = 0$. Since $P((X-1)^2)$ is monic and of degree $\varphi(k)$, it follows that

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

But 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 k roots of unity different from 1 and -1 for $k > 2$, a contradiction. $\square$

To obtain a solution to (1), we now fix values of a. Notice that this leads to $\Delta = t^2 - 4q = -4a = -f^2 D$ 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:

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

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

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

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 untractable.

procedure SMALLK(k, L)
  for $a := 1..a_{\max}$ **do**
    1. factor $R_k(a)$;
    2. **if** $R_k(a)$ has a prime factor $\ell \geq L$ **then**
      2.1 compute a root n of $\gcd(P_k(X), Q(X,a)) \bmod \ell$;
      2.2 **for** $s := 0..s_{\max}$ **do**
        if $a \leq n + s\ell$ **then**
          – compute $p = (n+s\ell)^2 + a$ or $p = (n+s\ell)^2 + (n+s\ell) + a$, respectively, depending on the choice of R_k;
          – **if** p is prime **then** compute E;

Remarks:

- Any number congruent to n modulo ℓ can be used in its place, this is why we consider small values of s in 2.2.

- At point 2.2, we do not need a to be squarefree. Indeed, we may write $4a = f^2 D$ where $-D$ is some fundamental discriminant and build E having CM by the principal order. This means that we could loop over (D, f) rather than over a, so as to keep D in a desired range.

- At 2.1, we do not really need ℓ to be prime. Replacing by a multiple of it works as well.

- Factoring $R_k(a)$ can be done with a large sieve, reminiscent of the NFS algorithm. In practice, we are happy with using a bound B and finding values of $R_k(a)$ which are composed of small primes below B and a large prime cofactor.

- We generally do not start at $a = 1$; as a matter of fact, since $R_k(a) \sim (4a)^{\varphi(k)}$ and R_k is increasing, we first compute the smallest a such that $R_k(a) \geq L$. We would like to keep $R_k(a)$ close to L. This can be impossible when $\varphi(k)$ is too large. For instance, if $12^{\varphi(k)} \gg L$, then all values of a larger than 3 will yield huge values of $R_k(a)$ for which finding prime factors of size $\log L$ would be very difficult (see the example with $k = 50$ below).

3.4 Heuristics

Let us sketch a rough analysis of our algorithm. We assume in a restricted model that we require $R_k(a)$ to be prime and assume this happens with probability $O(1/\log L)$. The integer n has a size of roughly L and p will be prime with probability $O(1/\log L)$, too. This means that we should find suitable solutions with probability $O(1/\log^2 L)$.

4 Numerical examples

To demonstrate our ideas, we have implemented the search for suitable CM parameters of elliptic curves in MAGMA[7]. The time needed to generate parameters for a curve of cryptographic size (160 to 200 bits) ranges from 1.5 seconds for $k = 12$ to about 30 seconds for $k = 50$, on a Pentium III running at 450 MHz. The corresponding CM curves $Y^2 = X^3 + AX + B$ were then constructed with our own C++ program relying on GMP[14], MPFR[16], MPC[13] and NTL[27]. The running times r provided in seconds are those for the curve construction on a Pentium III with 800 MHz. Unless otherwise stated, $t = +2n$. We first give a few small examples for the first prime values of k. Let us start with $k = 5$:

$$
\begin{aligned}
a &= 26103 \\
D &= 26103 \\
h &= 88 \\
p &= n^2 + a = 10316095101096156580609884521822230897927 \\
\ell &= 118856368237249643641 \\
A &= 6361774565981298467679675481620482961778 \\
B &= 7679881411019584505323078495021065607161 \\
r &= 1.2 \text{ sec}
\end{aligned}
$$

With $k = 7$:

$$
\begin{aligned}
a &= 1068 \\
D &= 267 \\
h &= 2 \\
p &= n^2 + a = 22280215019917539692076037201942564656877 \\
\ell &= 209942810985515700149 \\
A &= 20081485727637137786281947313744519173193 \\
B &= 19348575963543670484350584017678504011965 \\
r &= 0.5 \text{ sec}
\end{aligned}
$$

The following are examples of cryptographic size parameters:

$$
\begin{aligned}
k &= 10 \\
a &= 163841^2 \cdot 381535 \\
D &= 381535 \\
h &= 304 \\
p &= n^2 + a \\
&= 3841473059399107170103126625214956243555849230586730206554319192403126758\backslash \\
&\quad 24784619950343423791044836076585229766559410700100854819 \text{ (428 bits)} \\
\ell &= 4686879083953795487935291153103592178053824492905821016357311641 \text{ (212 bits)} \\
A &= 3614578796541747106204758437452623506218014739109496255047150073038238\backslash \\
&\quad 74440660375308333064155960208871834107728173994725817706209 \\
B &= 9779653359898889715032179580552084314015037548925981335085475716478582\backslash \\
&\quad 3429429213794100661750235442419193580537672582267656086793 \\
r &= 57 \text{ sec}
\end{aligned}
$$

$$
\begin{aligned}
k &= 11\\
a &= 3432987\\
D &= 13731947\\
h &= 675\\
p &= n^2+n+a\\
&= 1085821608657960459200424901105246469500036293041071392729642052706715552\backslash\\
&\ 5209414077340531489889487980320059886340361265142418889395568109\ \text{(452 bits)}\\
t &= +2n+1\\
\ell &= 318685188024102758902344691420660823461423047681320078259503739866651\ \text{(225 bits)}\\
A &= 1559295546932200357119739705088716590408695933963361975762035466055625821\backslash\\
&\ 563020387825392942383755862763911883552315027999018090902306395\\
B &= 9317871453629336870829152280819931917211836532224958585880327639452271445\backslash\\
&\ 556969901994211583104666470565255768963327547426970047466787266\\
r &= 190\ \text{sec}
\end{aligned}
$$

The last example, for $k = 50$, illustrates what happens when k is large. Then even the smallest values of $R_k(a)$ will be large, and the prime factors we can get also. Here, L was chosen to be 2^{200} and the first a found after a reasonable amount of time was large (ℓ has more than 800 bits):

$$
\begin{aligned}
a &= 3717^2 \cdot 100031\\
D &= 100031\\
h &= 360\\
p &= n^2+a\\
&= 2084292065314179094038505383926223683700428038066209523757745389853 2012669\backslash\\
&\ 1227876716876888564903033968788419500249219798452103104756973894831 4071100\backslash\\
&\ 6477334297523032986215627111710574173903692412752701919385129216682 4743040\backslash\\
&\ 1758989985763454227102619359018889280821444962007517094471923620395 5726821\backslash\\
&\ 0309100849868079249091307188331236661389291161507599626974026073275 0552134\backslash\\
&\ 8111348972454845217360182425166251283520826888354484840630216919352 5823153\backslash\\
&\ 20827704918947427827341111530920345812116928310854478407406457 2363\ \text{(1698 bits)}\\
\ell &= 1421099460489807177516490307596904251717131324451350726272701699909 1734563\backslash\\
&\ 9710146961151137455952738914556306194330933966571782976558849649815 8653799\backslash\\
&\ 5162073226551332737421827771070040483868925894621874717722494381552 0597387\backslash\\
&\ 891445377017922059001106955159901\ \text{(849 bits)}\\
A &= 1515618644722883998752841153504394941363739943634614030790966601389 6538378\backslash\\
&\ 3363819915468509783159293956991191159636109517149473771367073867342 0839041\backslash\\
&\ 9838046418721856278715617332253449742051072929172521135740148892388 4852083\backslash\\
&\ 9263769083282573290715483379554112379582110849258114814253385941455 4476338\backslash\\
&\ 0642451020309440540034283968282096233217355950883619113807363824272 5941450\backslash\\
&\ 5537093703811169204177426687074566598201138313780584583245159403708 9761358\backslash\\
&\ 57979558975576399388969281527931469742364199374858477874960707 1723\\
B &= 6312968160877259356447846153883774660180345661353456918827918752840 7093916\backslash\\
&\ 9998420760400873342770359634626418793486661572312296253181158932351 7379888\backslash\\
&\ 7991723599471197141437383685308835401323022970615602347301123787296 6407517\backslash\\
&\ 8456987872011282362188982667262236522285178243391416893565655083435 4839033\backslash\\
&\ 9838674605005345539848404988219705366969471601730924004271343835134 2205108\backslash\\
&\ 6418922901116621273297806326552546085876331594711228839067345920435 7997093\backslash\\
&\ 00876086881369139670649676832950624484076469592416515616766380722\\
r &= 1500\ \text{sec}
\end{aligned}
$$

5 Cryptographic implications

Our method yields elliptic curves E defined over a prime field $\mathbb{F}_p$ having a subgroup of prime order ℓ of size $O(\sqrt{p})$, which is easily seen from equation (1). Roughly speaking, a secure $\ell = 2^{200}$ implies a field of size 2^{400}. Note that we implicitely 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 problem can be solved for fixed q and prime curve order m.

6 Conclusions

Our method cannot reach a fixed prime power q, but replaces this with a large variety of primes to show up during the computations. More work is needed to improve this situation.

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

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. of Cryptology*, 11:141–145, 1998.

[3] P. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees, 2002. Available at `http://eprint.iacr.org/2002/089/`.

[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 Comput. Sci.*, pages 213–229. Springer-Verlag, 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 Comput. Sci.*, pages 514–532. Springer-Verlag, 2001.

[6] J. Cha and J. Cheon. Identity-based signature from the Weil pairing. Available at `http://vega.icu.ac.kr/~jhcheon/publications.html`, 2002.

[7] Computational Algebra Group of the University of Sydney. MAGMA version 2.9, 2001. `http://magma.maths.usyd.edu.au/magma/`.

[8] D. A. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons, 1989.

[9] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics.* Springer–Verlag, 2nd edition, 1980.

[10] R. Dupont and A. Enge. Practical and secure non-interactive key distribution based on pairings, 2002. Draft.

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

[12] A. Enge and R. Schertz. Constructing elliptic curves from modular curves of positive genus. In preparation, 2001.

[13] A. Enge and P. Zimmermann. MPC — Multiprecision Complex arithmetic library version 0.1, 2002. Available at `http://www.loria.fr/~zimmerma/free/`.

[14] T. Granlund et al. GMP — GNU Multiprecision library version 4.1, 2002. Available at `http://www.swox.com/gmp/`.

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

[16] G. Hanrot, V. Lefèvre, and P. Zimmermann et al. MPFR — Multiprecision Floating point library with exact Rounding version 2.0.1, 2002. Available at `http://www.mpfr.org/`.

[17] F. Hess. Exponent group signature schemes and efficient identity based signature schemes based on pairings. Cryptology ePrint Archive, Report 2002/012, available at `http://eprint.iacr.org/2002/012/`.

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

[19] 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 Comput. Sci.*, pages 250–263. Springer-Verlag, 1994.

[20] 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.

[21] V. Miller. Short programs for functions on curves. Draft, 1986.

[22] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, E84-A(5), May 2001.

[23] F. Morain. Building cyclic elliptic curves modulo large primes. In D. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 328–336. Springer–Verlag, 1991.

[24] K. Paterson. Id-based signatures form pairings on elliptic curves, 2002. Available at `http://www.eprint.iacr.org/2002/004`.

[25] C. Pomerance. Very short primality proofs. *Math. Comp.*, 48(177):315–322, 1987.

[26] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. SCIS 2000, The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26–28.

[27] V. Shoup. NTL — Number Theory Library 5.2, 2001. Available at `http://shoup.net/ntl/`.

[28] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Grad. Texts in Math.* Springer-Verlag, 1994.

[29] N. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. To appear in Electronics Letters, 2001.