Pairings on elliptic curves over finite commutative rings

Steven D. Galbraith and James F. McKee*

Department of Mathematics,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, UK.
[Steven.Galbraith,James.McKee]@rhul.ac.uk

Abstract. The Weil and Tate pairings are defined for elliptic curves over fields, including finite fields. These definitions extend naturally to elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, for any positive integer N, or more generally to elliptic curves over any finite commutative ring, and even the reduced Tate pairing makes sense in this more general setting.
This paper discusses a number of issues which arise if one tries to develop pairing-based cryptosystems on elliptic curves over such rings. We argue that, although it may be possible to develop some cryptosystems in this setting, there are obstacles in adapting many of the main ideas in pairing-based cryptography to elliptic curves over rings.
Our main results are: (i) an oracle that computes reduced Tate pairings over such rings (or even just over $\mathbb{Z}/N\mathbb{Z}$) can be used to factorise integers; and (ii) an oracle that determines whether or not the reduced Tate pairing of two points is trivial can be used to solve the quadratic residuosity problem.
Keywords: Elliptic curves modulo N, pairings, integer factorisation, quadratic residuosity.

1 Introduction

Pairings are a major topic in elliptic curve public key cryptography, following the success of cryptosystems such as Joux's three-party key exchange protocol [10] and the Boneh-Franklin identity-based encryption scheme [1]. Recall that if E is an elliptic curve over a field K and if r is coprime to the characteristic of K then the Weil pairing maps $E[r] \times E[r]$ to μ_r, where μ_r is the group of r-th roots of unity in the field $\overline{K}$. The Tate pairing [5, 6] is usually used in practical implementations for efficiency reasons, though it is necessary to consider the so-called reduced Tate pairing which takes values in μ_r.

Elliptic curves modulo composite integers N have also been proposed for cryptography. The motivation is that security can also rely on the integer factorisation problem and that new functionalities might be possible due to the extra trapdoor. It is therefore a natural problem to try to develop pairing-based

* This research was funded by EPSRC grant GR/R84375.

cryptosystems on elliptic curves modulo composite integers N. The fundamental question is whether pairings can be computed on elliptic curves over rings, and whether other aspects of pairing-based cryptography can be generalised to this situation. Indeed, the first author has been asked by several researchers whether this is possible.

We might imagine a system in which the factorisation of N is secret, but N is public, and a user is required to compute a pairing on some elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ (or some extension ring). The security of the cryptosystem is presumed to rely on the hardness of factoring and possibly some other computational problems.

We will explain that the Weil pairing can be computed successfully in this setting (as long as certain data is provided). On the other hand, we show in Theorem 3 that the reduced Tate pairing cannot be computed without knowing the factorisation of N. As a companion to this result we show in Theorem 4 that even just being able to detect whether or not the reduced Tate pairing of two points is trivial would allow one to solve the quadratic residuosity problem. We will also argue that certain operations which are essential to many pairing-based cryptosystems (such as hashing to a point) cannot be performed with elliptic curves over rings if the factorisation is unknown.

Our opinion is that the use of pairings on elliptic curves over rings will not be as successful as the case of elliptic curves over finite fields. We believe that the potential secure and practical applications are, at best, limited to a few special situations. One might imagine, for example, a scheme where only the holder of secret information is supposed to be able to compute pairings.

The structure of the paper is as follows. We recall some results for elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, making some observations concerning quadratic residuosity and the natural generalisations to finite extensions of $\mathbb{Z}/N\mathbb{Z}$. There follows an example which introduces some of the issues which arise when considering pairings on elliptic curves over rings. In particular, there are issues concerning the splitting of $N = pq$ where $p - 1$ and $q - 1$ (or $p + 1$ and $q + 1$) share some common factor: we recall some techniques for integer factorisation of numbers of this form. Then we gather some well-known results concerning the equivalence of factoring and extracting roots, put in the setting of surjective homomorphisms from $(\mathbb{Z}/N\mathbb{Z})^*$ to roots of unity. We then define what we mean by pairings for elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ and over more general finite commutative rings, and prove the results stated above (Theorems 3 and 4).

When giving complexity estimates for algorithms over $\mathbb{Z}/N\mathbb{Z}$, the computation of the greatest common divisor of two numbers between 1 and N is counted as a single 'ring operation'.

2 Elliptic curves modulo N

Let N be an integer greater than 1 with $\gcd(N, 6) = 1$ (this restriction on N is not essential, but it simplifies the exposition in places). An elliptic curve E over the ring $\mathbb{Z}/N\mathbb{Z}$ is the set of solutions $(x : y : z)$ in projective space over $\mathbb{Z}/N\mathbb{Z}$

(insisting that $\gcd(x, y, z, N) = 1$) to a Weierstrass equation

$$y^2 z = x^3 + a_4 x z^2 + a_6 z^3 \,, \tag{1}$$

where the discriminant of the cubic on the right, namely $4a_4^3 + 27a_6^2$, has no prime factor in common with N. There is a group law on $E(\mathbb{Z}/N\mathbb{Z})$ given by explicit formulae which can be computed without knowledge of the factorisation of N. The identity element is $0 = (0 : 1 : 0)$. We refer to Lenstra [13, 14] for details about elliptic curves over rings.

If the prime factorisation of N is $N = \prod_{i=1}^{m} p_i^{a_i}$, then $E(\mathbb{Z}/N\mathbb{Z})$ is isomorphic as a group to the direct product of elliptic curve groups $\prod_{i=1}^{m} E(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$. If we let E_i be the reduction of E modulo p_i, then E_i is an elliptic curve over the field $\mathbb{F}_{p_i}$. One finds that

$$\#E(\mathbb{Z}/p_i^{a_i}\mathbb{Z}) = p_i^{a_i - 1} \#E_i(\mathbb{F}_{p_i})$$

(see, for example, [7]).

The first proposal to base cryptosystems on elliptic curves over the ring $\mathbb{Z}/N\mathbb{Z}$ was by Koyama, Maurer, Okamoto and Vanstone [12]. Other proposals have been given by Demytko [4], Meyer and Mueller [21], and Vanstone and Zuccherato [31]. The security of such cryptosystems is related to the difficulty of factorising N.

The following theorem was established in [11].

Theorem 1. *Let N be a composite integer satisfying $\gcd(N, 6) = 1$. Given an oracle that takes as its input an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, and outputs the number of points on the curve, one can factorise N in random polynomial time.*

We remark that an oracle that merely tells us whether or not two elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ have the same number of points can be used to solve the quadratic residuosity problem.

Theorem 2. *Suppose that $\mathcal{O}$ is an oracle that determines whether or not two elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ have the same number of points. Let $a \in (\mathbb{Z}/N\mathbb{Z})^*$ be such that $\left(\frac{a}{N}\right) = 1$. Then there is a randomised polynomial time algorithm that makes one call to the oracle and returns a guess as to whether or not a is actually a square in $(\mathbb{Z}/N\mathbb{Z})^*$, with the following probabilities of success:*

- *if a is a square in $(\mathbb{Z}/N\mathbb{Z})^*$, then the algorithm will return the guess 'square';*
- *if a is not a square in $(\mathbb{Z}/N\mathbb{Z})^*$, then the algorithm will return the guess 'not a square' with probability $1 - \epsilon$, where*

$$\epsilon = O(\log p \log\log p / \sqrt{p}) \,,$$

with p being any prime dividing N such that $\left(\frac{a}{p}\right) = -1$.

Proof. Suppose that we are given $a \in (\mathbb{Z}/N\mathbb{Z})^*$ with $\left(\frac{a}{N}\right) = 1$. We choose random a_4, a_6 in $\mathbb{Z}/N\mathbb{Z}$ such that equation (1) defines an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$. If a is a square in $(\mathbb{Z}/N\mathbb{Z})^*$, then the twisted curve $E^{(a)}$ with equation

$$y^2 z = x^3 + a_4 a^2 x z^2 + a_6 a^3 z^3$$

has the same number of points as E. Otherwise, let p be any prime dividing N such that $\left(\frac{a}{p}\right) = -1$. Suppose that $N = p^r n$, with $\gcd(p, n) = 1$. We can write the number of points on E over $\mathbb{Z}/N\mathbb{Z}$ as

$$\#E(\mathbb{Z}/N\mathbb{Z}) = (p + 1 - t)m_1 \,,$$

where $p + 1 - t = \#E(\mathbb{Z}/p\mathbb{Z})$ and $m_1 = p^{r-1}\#E(\mathbb{Z}/n\mathbb{Z})$. Then the number of points on $E^{(a)}$ is

$$\#E^{(a)}(\mathbb{Z}/N\mathbb{Z}) = (p + 1 + t)m_2 \,,$$

where $m_2 = p^{r-1}\#E^{(a)}(\mathbb{Z}/n\mathbb{Z})$. The numbers of points on E and $E^{(a)}$ are different unless

$$t = (p + 1)(m_1 - m_2)/(m_1 + m_2) \,.$$

Conditioning on the value of the pair (m_1, m_2) this value of t occurs with probability

$$O(\log p \log\log p/\sqrt{p})$$

(Theorem 2 in [18]). The implied constant here is absolute, not depending on (m_1, m_2), or on a. The result follows immediately. □

More generally, one might not have access to an oracle as in Theorems 1 and 2, but might simply be given a single elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ with a known number of points, M. Two complementary approaches for attempting to factorise N from this limited information have appeared in the literature:

1. One method is to multiply a point on a random quadratic twist by M. In general, it is hard to find points in $E(\mathbb{Z}/N\mathbb{Z})$ (for example, choosing an x-coordinate, putting $z = 1$, and solving for y requires taking a square root). However, there are formulae for performing point multiplications which use x-coordinates only (on the affine piece $z = 1$: see the *Formulary* of Cassels, and the exercises at the end of chapter 26, in [3]).
   A random $x \in \mathbb{Z}/N\mathbb{Z}$ is the x-coordinate of a point $(x : y : 1)$ on E_i with probability roughly $1/2$. If this is the case then $M(x : y : 1) = 0$ on E_i. On the other hand, if x is not a valid x-coordinate then there is a corresponding point $(x : y : 1)$ on a quadratic twist $E^{(d)}$ over $\mathbb{F}_{p_i}$ and for most curves we would not expect $M(x : y : 1) = 0$ on $E^{(d)}(\mathbb{F}_{p_i})$.
   The algorithm to factorise N is to take random x-coordinates (with $z = 1$) and to multiply by M, using x-coordinates only. With high probability the resulting point will be the identity modulo some, but not all, primes p dividing N. So taking the gcd of the resulting z-coordinate with N will split N. Details of this method are given in Okamoto and Uchiyama [24].
2. Another way to obtain this result is to mimic the standard randomised reduction from knowing $\#(\mathbb{Z}/N\mathbb{Z})^*$ to factoring (similar to the Miller-Rabin primality test). We write

$$M = \#E(\mathbb{Z}/N\mathbb{Z}) = 2^m M'$$

where M' is odd. We then choose random x-coordinates (with $z = 1$) and multiply by M' and then compute the sequence of doublings of this point. The details are given in [17]. In [11] it is noted that the prime 2 can be replaced by a larger prime.

3 Extension rings

In practice, especially when considering pairings, we may be interested in extending our ring $\mathbb{Z}/N\mathbb{Z}$. For example, we may wish to force the full r-torsion onto our curve for some r. To this end we consider elliptic curves over rings of the form

$$R_{N,f} = (\mathbb{Z}/N\mathbb{Z})[x]/(f(x)) \,,$$

where $f(x)$ is some polynomial in $(\mathbb{Z}/N\mathbb{Z})[x]$. The splitting of $f(x)$ may be different modulo different prime divisors of N. The above results readily extend to this setting, twisting by random elements of R. If N is squarefree, and $f(x)$ is squarefree modulo every prime dividing N, then $R = R_{N,f}$ is a product of finite fields.

4 An example

To clarify the discussion above, and to introduce some of the issues which arise when considering pairings, we give an example.

Let p_1, p_2 be primes congruent to 2 modulo 3 and let r be a prime such that $r \mid (p_i + 1)$, $r^2 \nmid (p_i + 1)$ for $i = 1, 2$. Let E be the elliptic curve $y^2 = x^3 + 1$. For each $i = 1, 2$ let E_i be the reduction of E modulo p_i. It is well known that E_i is supersingular, that $\#E(\mathbb{F}_{p_i}) = p_i + 1$, and that $E[r] \subset E(\mathbb{F}_{p_i^2})$. Let $P, Q \in E_i[r]$. Then the Weil (or reduced Tate) pairing gives an r-th root of unity

$$e_r(P, Q) \in \mathbb{F}_{p_i^2}^* \,.$$

The field $\mathbb{F}_{p_i^2}$ can be defined as $\mathbb{F}_{p_i}(\theta)$ where $\theta^2 + \theta + 1 = 0$. If P and Q are points of order r such that $P \neq 0$ lies in $E_i(\mathbb{F}_{p_i})$ and Q does not lie in $E(\mathbb{F}_{p_i})$ then it is easy to show that $e_r(P, Q) \neq 1$.

Define $N = p_1 p_2$ and define the ring

$$R = (\mathbb{Z}/N\mathbb{Z})[\theta]/(\theta^2 + \theta + 1) \,.$$

Then

$$R \cong \mathbb{F}_{p_1^2} \times \mathbb{F}_{p_2^2} \,.$$

Let E be the elliptic curve above. Then

$$\#E(R) = (p_1 + 1)^2 (p_2 + 1)^2 \,.$$

Note that there seems to be no reason to use large embedding degrees for elliptic curves over rings since the ground ring is already large due to the factoring

problem. Indeed, one might prefer embedding degree 1, but then $r \mid (p_i - 1)$, and in the case of the Weil pairing also $r^2 \mid \#E(\mathbb{F}_{p_i})$, for each prime p_i dividing N, and so the attacks of Section 5 must be borne in mind.

Let P and Q be points of order r in $E(R)$ such that $P \neq 0$ lies in $E(\mathbb{Z}/N\mathbb{Z})$ and $Q \notin E(\mathbb{Z}/N\mathbb{Z})$. Then, as before, $e_r(P, Q)$ is a non-trivial r-th root of unity in R^*. The distortion map

$$\psi(x, y) = (\theta x, y)$$

can be used to map points $P \in E(\mathbb{Z}/N\mathbb{Z})$ into points in $E(R)$ and so we can obtain a non-trivial pairing between points of order r in $E(\mathbb{Z}/N\mathbb{Z})$.

We will argue in Section 8 that the reduced Tate pairing cannot be computed without knowing the factorisation of N. But, if E, R, P, Q and r are given, then one can compute the Weil pairing using Miller's algorithm [22, 23] as

$$e_r(P, Q) = (-1)^r F_{r,P}(Q)/F_{r,Q}(P)$$

without knowing the factorisation of N, where $F_{r,P}$ is a function on E with divisor

$$(F_{r,P}) = r(P) - r(0)$$

(see [23]).

Hence, one can solve decision Diffie-Hellman problems in $E[r]$ and one can implement Joux's three-party key exchange protocol [10] in this setting. It is therefore plausible that cryptosystems can be developed based on elliptic curves over rings which exploit both the hardness of the integer factorisation problem as well as aspects of pairing-based cryptography. Such systems might have potential functionalities which cannot be realised using elliptic curves over finite fields.

However, there are a number of issues which differ from the case of elliptic curves over finite fields which should be considered before one can develop such cryptosystems:

- The value r must play a symmetric role for all primes $p_i \mid N$.
  For example, if $\zeta \in R^*$ is such that $\zeta \pmod{p_1}$ has order r but $\zeta \equiv 1 \pmod{p_2}$ then one can split N by computing $\gcd(\zeta - 1, N)$. Similarly, if P is a point which has order r on E_1 but order coprime to r on E_2 then one can split N by multiplying E by r and computing gcds.
- The point order r must be provided to compute pairings.
  This is because Miller's algorithm essentially involves the operation of point multiplication by r. We know of no way to compute pairings if r is not provided. Since we are obliged to use the Weil pairing, both points must have order r. The information on r can be used to improve certain factoring algorithms (see Section 5 below). Hence, r should be chosen to be much smaller than the primes p_i (for the above example we would recommend choosing r to have 160 bits and the p_i to have at least 512 bits).
- Generating points on elliptic curves over rings is a hard problem.
  This is not an obstacle to a cryptosystem such as Joux's three-party key exchange if a base-point P is included in the system parameters. However, for

some protocols it may be necessary for users to find random points $Q \in E(R)$ without simply multiplying an existing point by some integer.
There are two traditional solutions to this problem. The first, used in the KMOV cryptosystem [12], is to choose $P = (x_P, y_P)$ and to modify the curve equation so that P lies on E. This solution could be used in pairing applications, though note that it does not preserve existing points. The second solution, due to Demytko [4], is to work with x-coordinates only. It is not possible to compute pairings exactly using x-coordinates only, but it may be possible to compute traces of pairings, as done by Scott and Barreto [28]. A different solution is to choose x_P and extend the ring as $R' = R(\sqrt{x_P^3 + a_4 x_P + a_6})$. It is unclear whether any of these solutions would be practical for pairing-based cryptosystems.

– Hashing to a point of order r is hard.
In many pairing-based cryptosystems it is necessary to hash to a point of order r. The hashing process first involves finding a random point in $E(R)$, which as mentioned above is already a potential difficulty. Further, to obtain a point of exact order r it is necessary to multiply the point by a cofactor m. Since r is public then, once m is also given, the exponent of the group $E(R)$ or $E(\mathbb{Z}/N\mathbb{Z})$ is known, and we can therefore hope to factorise N using the methods discussed at the end of Section 2.
Due to this issue, it seems unlikely that cryptosystems such as the Boneh-Franklin identity-based encryption scheme [1] or the Boneh-Lynn-Shacham signature scheme [2] can be developed for elliptic curves over extensions of $\mathbb{Z}/N\mathbb{Z}$ without revealing the factorisation of N.

5 Factoring if r is known

From time to time (e.g., [9], [15]) authors propose variants of RSA, with or without elliptic curves, in which $N = pq$ and there is some r greater than 1 such that both $r \mid (p-1)$ and $r \mid (q-1)$. If r is small, then it cannot be kept secret, as observed in [20]: it will be a factor of $N - 1$, and Lenstra's Elliptic Curve Method [13] or Pollard's ρ method [25] can be used to recover r. Even if r is secret, it cannot be too large: applying Pollard's ρ method with the 'random' map

$$x \mapsto x^{N-1} + 1 \pmod{N}$$

will produce a sequence that repeats modulo p after $O(\sqrt{p/r})$ terms, on average (this observation also appeared in [20]), so that if r is too large then the factorisation of N will be found.

If r is known, then more powerful factorisation attacks are possible. Let us assume that $N = pq$ with p and q of similar size. Following [20], we can now employ a variant of Lehmer's method (described in [19]). Write

$$p = xr + 1\,, \quad q = yr + 1\,.$$

Then

$$(N-1)/r = xyr + (x+y) = ur + v$$

where u and v ($0 \le v < r$) are known and x, y are unknown. We have

$$x + y = v + cr\,, \quad xy = u - c\,,$$

where c is the (unknown) carry in expressing $(N-1)/r$ in base r as above. Since $cr \le x + y$ and both x and y are of size about $\sqrt{N}/r$, there are of order $\sqrt{N}/r^2$ values of c to test. A candidate for c can be tested quickly, since

$$r^2c^2 + (2rv + 4)c + v^2 - 4u = (x - y)^2$$

must be a square.

Again following [20] (see also [16] for the same idea in a different setting), we can improve this $O(\sqrt{N}/r^2)$ attack to one that takes only $O(N^{1/4}/r)$ ring operations (still assuming that $N = pq$ with p and q roughly equal). Note that the price for this improvement in speed is either to have increased storage or a heuristic algorithm. We observe that the exponent of $(\mathbb{Z}/N\mathbb{Z})^*$ is given by

$$\operatorname{lcm}(p - 1, q - 1) = \operatorname{lcm}(xr, yr)\,,$$

and so divides xyr. Take random $a \in (\mathbb{Z}/N\mathbb{Z})^*$. Then

$$a^{ur} = a^{xyr+cr} = a^{cr}\,.$$

Putting $b = a^r$, we have

$$b^u = b^c$$

in $(\mathbb{Z}/N\mathbb{Z})^*$. Since c has magnitude $\sqrt{N}/r^2$, we can recover c (modulo the order of b, which with high probability will have order nearly as large as $xy \approx N/r^2$) in $O(N^{1/4}/r)$ ring operations, either using the baby-step giant-step method of Shanks [29] or Pollard's λ method [26].

Similar remarks hold if both $r \mid (p+1)$ and $r \mid (q+1)$, as in Section 4. Small r can be spotted as a factor of $N - 1$. Large r make N vulnerable to Pollard's ρ method with the map

$$x \mapsto x^{N-1} + 1 \pmod N\,.$$

If r is known, we can determine $q + p$ modulo r^2, and hence perform a similar attack to the above that will split N in $O(N^{1/4}/r)$ ring operations if p and q are of similar size.

Finally in this context we should consider the implications of knowing a divisor d of the group order of $E(\mathbb{Z}/N\mathbb{Z})$. From Section 2, we must imagine that the group order M is secret. We might hope to split N using Lenstra's Elliptic Curve Method [13] or Pollard's λ method [26], with the curve E and the base point $d(x : y : 1)$ for random x. The worst case complexity of these attacks is

$$O\left(\min_{p|n} \sqrt{\#E(\mathbb{F}_p)/\gcd(d, \#E(\mathbb{F}_p))}\right)$$

ring operations.

6 Computing a surjective homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to certain roots of unity is as hard as factoring

It is well-known that computing square-roots modulo a composite is as hard as factoring [27], and indeed the same applies to rth roots if r is not too large and

$$\gcd(r, p-1) > 1$$

for some prime p dividing N. The ability to extract rth roots modulo N implies the ability to generate random rth roots of unity, and it is of course the latter that allows us to split N. We record these remarks here in a few Lemmas.

Let $N > 1$ be an odd integer that is not a prime power, and let $r > 1$ be any integer. Let $G_{N,r}$ be the unique maximal subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ having exponent dividing r, i.e.,

$$G_{N,r} = \{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^r = 1\}.$$

Another way of saying this is that $G_{N,r}$ contains all the rth roots of unity in $(\mathbb{Z}/N\mathbb{Z})^*$.

Any oracle which computes a surjective group homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$ can be used to factor N if r is not too large and $G_{N,r}$ is non-trivial: this statement is made precise in the Lemmas below. The homomorphic property simply ensures that the preimage of each element of $G_{N,r}$ is the same size: any map with this property, or something close to it, would suffice.

Let $\mathcal{O}(N, r, a)$ be an oracle which takes as input integers N and r and an element $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and returns the image of a under a surjective group homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$, where the homomorphism depends on N and r, but not a.

For example, if N is squarefree and $r \mid (p_i - 1)$ for all i then $\mathcal{O}(N, r, a)$ might return the Chinese remainder of the values

$$a^{(p_i-1)/r} \pmod{p_i}$$

for $1 \le i \le m$ (but any surjective homomorphism would do). In the case $r = 2$ and N odd and squarefree, this particular choice of oracle returns the Chinese remainder of the Legendre symbols for all p dividing N. We stress that this is not the same thing as the Jacobi symbol (which is the product of the Legendre symbols, and does not give a surjective homomorphism to $G_{N,2}$).

In the following Lemmas, we fix the notation

$$N = \prod_{i=1}^{m} p_i^{a_i}, \tag{2}$$

where $p_1, \ldots p_m$ are distinct odd primes, and $m \ge 2$. Then

$$G_{N,r} \cong \prod_{i=1}^{m} G_i, \tag{3}$$

where each G_i is cyclic of order dividing r.

Lemma 1. *Let N be as in (2) and let r be a positive integer greater than 1 such that*

$$r \mid p^{a_i-1}(p_i - 1)$$

for $1 \leq i \leq m$. Let $\mathcal{O}$ be an oracle computing a surjective homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$.

There is a randomised algorithm with negligible storage that will find a non-trivial factorisation of N in expected time $O(r)$ ring operations, using $O(r)$ oracle calls, on average.

Proof. The algorithm is simply to choose random $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and to obtain

$$b = \mathcal{O}(N, r, a)\,.$$

One can then compute $\gcd(b-1, N)$. This will split N as long as there are two primes p and q dividing N such that

$$b \equiv 1 \pmod{p} \quad \text{but } b \not\equiv 1 \pmod{q}\,.$$

In (3), each G_i now has order r. Of the r^2 possibilities for the image of a in $G_1 \times G_2$, $2(r-1)$ of them will split N, regardless of the image of a in the other G_i $(3 \leq i \leq m)$. For random a, the probability that we split N is therefore at least $2(r-1)/r^2$, so that the expected number of oracle calls is $O(r)$. □

The running time of the above algorithm can be reduced at the expense of some storage.

Lemma 2. *Let N be as in (2) and let r be a positive integer greater than 1 such that*

$$r \mid p_i^{a_i-1}(p_i - 1)$$

for $1 \leq i \leq m$. Let $\mathcal{O}$ be an oracle computing a surjective homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$.

There is a randomised algorithm requiring $O(\sqrt{r}\log N)$ storage that will find a non-trivial factorisation of N in expected time $O(\sqrt{r}\log r \log\log r)$ ring operations, using $O(\sqrt{r})$ oracle calls, on average.

Proof. The algorithm chooses random $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and forms a list of values $\mathcal{O}(N, r, a)$. When the list has length $O(\sqrt{r})$, one checks for repeats in the list modulo some but not all prime factors of N by standard fast polynomial evaluation techniques [30]. It is likely that there is a repeat modulo some prime dividing N whilst being very unlikely that there is a repeat modulo N. If r is not known, or if no repeat has been found, one can repeatedly double the length of the list until success. □

With the extra hypothesis that $\mathcal{O}(N, r, a) \pmod{p}$ depends only on $a \pmod{p}$, there is a low-storage variant using Pollard's ρ method [25]. Not all homomorphic oracles have this property. For example, with $N = pq$ and $r = 2$, we could perversely map a to the Chinese remainder of

$$\left(\frac{a}{p}\right) \pmod{q} \quad \text{and} \quad \left(\frac{a}{q}\right) \pmod{p}\,.$$

Lemma 3. *Let N be as in (2) and let r be a positive integer greater than 1 such that*

$$r \mid p_i^{a_i-1}(p_i - 1)$$

for $1 \leq i \leq m$. Let $\mathcal{O}$ be an oracle computing a surjective homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$ satisfying the additional property that $\mathcal{O}(N, r, a) \pmod p$ depends only on $a \pmod p$ (for each prime p dividing N).

There is a heuristic algorithm requiring negligible storage that will find a non-trivial factorisation of N in heuristic expected time $O(\sqrt{r})$ ring operations, using $O(\sqrt{r})$ oracle calls, on average.

Proof. Apply Pollard's ρ method [25] with the 'random' map

$$x \mapsto \mathcal{O}(N, r, x) + 1 \,.$$

(We add 1 to improve the pseudorandom behaviour of the map, by mixing addition with the multiplicative nature of our homomorphic oracle.) Described simply (but not optimally), we compute (but do not store) sequences x_n and $y_n = x_{2n}$, starting with (say) $x_0 = y_0 = 1$, and using the rule

$$x_{n+1} = \mathcal{O}(N, r, x_n) + 1 \,.$$

At each step we compute

$$\gcd(x_n - y_n, N)$$

until we find a non-trivial factor of N.

The complexity is as standard for Pollard's ρ method. □

The situation is of course much more trivial if r is a prime such that

$$r \mid p_i^{a_i-1}(p_i - 1)$$

for some but not all primes p_i dividing N.

Lemma 4. *Let N be as in (2) and let r be a prime such that*

$$r \mid p_i^{a_i-1}(p_i - 1)$$

for at least one but not all of the p_i. Let $\mathcal{O}$ be an oracle computing a surjective homomorphism from $(\mathbb{Z}/N\mathbb{Z})^*$ to $G_{N,r}$.

Then there is a randomised algorithm to find a non-trivial factorisation of N which runs in expected time $O(1)$ ring operations, using $O(1)$ oracle calls, on average.

Proof. The algorithm is simply to choose random $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and to obtain

$$b = \mathcal{O}(N, r, a) \,.$$

One can then compute

$$\gcd(b - 1, N) \,.$$

Since there is at least one prime p_i dividing N such that

$$r \nmid p_i^{a_i-1}(p_i - 1)$$

we know that

$$b \equiv 1 \pmod{p_i^{a_i}}\,.$$

Hence, all that is required is that

$$b \not\equiv 1 \pmod{p_j}$$

for some other prime p_j dividing N. The probability of this event is at least $(r-1)/r$, so that the expected number of oracle calls is at most 2. □

Similar results hold for the rings $R_{N,f}$, but the performance of the analogous algorithms has worse dependence on r. If the r-torsion of the p-component of $R_{N,f}$ has order r^{n_p} (for p a prime dividing N), then the expected running time for the analogue of Lemmas 1, 2 and 3 has r replaced by $r^{\min(n_p)}$. The analogue of Lemma 4 remains just as trivial.

The case $r = 2$ in Lemma 1 is particularly attractive, since if N is odd then we know that $r \mid (p-1)$ for all p dividing N.

7 The Tate pairing on curves over finite commutative rings

One of the main results of this paper is to argue that there is no way to compute reduced Tate pairings on general $E(\mathbb{Z}/N\mathbb{Z})$ without knowing the factorisation of N. We achieve this by showing that if $\mathcal{O}$ is an oracle for computing reduced Tate pairings on such curves then one can use $\mathcal{O}$ to factorise N.

We first recall the Tate pairing for elliptic curves over finite fields (see Frey and Rück [5, 6] for details). Let E be an elliptic curve over $\mathbb{F}_q$ (q being a power of a prime) and let r be coprime to q. Let $k \in \mathbb{N}$ be minimal such that $r \mid (q^k - 1)$. The integer k depends on both q and r (indeed, it is the order of q modulo r) and is often called the 'embedding degree'. Define by $E[r]$ the set of points $P \in E(\mathbb{F}_{q^k})$ such that $rP = 0$ (we assume that $\#E[r] > 1$). The Tate pairing is a non-degenerate pairing

$$\langle \cdot, \cdot \rangle_r : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r\,.$$

In practice the Tate pairing is computed using an algorithm due to Miller [22, 23]. If $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$ then there is a function $F_{r,P}$ having divisor

$$(F_{r,P}) = r(P) - r(0)\,.$$

Miller's algorithm builds up this function $F_{r,P}$ in stages in a way analogous to the double and add algorithm for point exponentiation. Then

$$\langle P, Q \rangle_r = F_{r,P}(Q + S)/F_{r,P}(S)$$

for a suitable auxiliary point $S \in E(\mathbb{F}_{q^k})$. Different choices of auxiliary point S will give different values in $\mathbb{F}_{q^k}^*$, but they are all equivalent in the quotient group $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$.

Henceforth we shall not insist that the values of r and k satisfy $r \mid (q^k - 1)$. Provided that $P \in E[r]$, and that we can find a suitable auxiliary point S, we can still perform Miller's algorithm. The pairing may no longer be non-degenerate, and of course

$$(\mathbb{F}_{q^k}^*)^r = (\mathbb{F}_{q^k}^*)^{\gcd(r, q^k-1)} .$$

Let $N = \prod_{i=1}^m p_i$ be a squarefree positive integer. As with other applications of elliptic curves, the natural way to generalise the Tate or Weil pairings to points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ is to use the Chinese remainder theorem to piece together the values of the pairing over $\mathbb{F}_p$ for the various p dividing N. If the factorisation of N is known, then of course this computation can be done. One can readily generalise this to curves over the rings $R_{N,f}$, considered in section 3, provided that $R_{N,f}$ is a product of fields. Further generalisations are considered below.

If the factorisation of N is not known, then one can still compute the Weil pairing (of points P and Q of known order), or the 'raw' Tate pairing (where only the order of P is needed) over $\mathbb{Z}/N\mathbb{Z}$ simply by following Miller's algorithm, working modulo N throughout.

For cryptographic applications the fact that the Tate pairing assumes values defined modulo rth powers is intolerable. Hence, returning first to the case of finite fields, one uses the 'reduced' Tate pairing

$$e(P, Q) = \langle P, Q \rangle_r^{(q^k-1)/\gcd(r, q^k-1)} .$$

There is some choice in how to generalise this reduced Tate pairing to elliptic curves over rings. We give two definitions below. We will show in Theorem 3 that (with either definition) computing the reduced Tate pairing is as hard as factoring.

For clarity, we give both definitions for the simplest case where N is squarefree and we do not extend the ring $\mathbb{Z}/N\mathbb{Z}$. Generalisations will be discussed immediately afterwards.

Definition 1. *Suppose that $N = \prod_{i=1}^m p_i$ is a squarefree positive integer, and that r is a positive integer. Let E be an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ defined by (1). Suppose that P and Q are points on E, with the order of P dividing r. Let $\langle P, Q \rangle_{r,i}$ be the raw Tate pairing of P and $Q + rE$ over $\mathbb{Z}/p_i\mathbb{Z}$. Define*

$$e_i(P, Q) = \langle P, Q \rangle_{r,i}^{(p_i-1)/\gcd(r, p_i-1)} .$$

Then the reduced Tate pairing $e(P, Q)$ is defined to be the unique element of $(\mathbb{Z}/N\mathbb{Z})^*$ satisfying

$$e(P, Q) \equiv e_i(P, Q) \pmod{p_i}$$

for each i ($1 \leq i \leq m$).

Definition 2. *Suppose that $N = \prod_{i=1}^{m} p_i$ is a squarefree positive integer, and that r is a positive integer. Let E be an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ defined by (1). Suppose that P and Q are points on E, with the order of P dividing r. Let $\langle P, Q\rangle_r$ be the raw Tate pairing of P and $Q + rE$ over $\mathbb{Z}/N\mathbb{Z}$. Then the reduced Tate pairing $e(P, Q)$ is defined by*

$$e(P, Q) = \langle P, Q\rangle_r^{g/\gcd(r,g)},$$

where g is the exponent of $(\mathbb{Z}/N\mathbb{Z})^*$.

The first definition seems more natural because it behaves well under reduction, but we recognise that there is a choice here.

If N is not squarefree, then $\mathbb{Z}/N\mathbb{Z}$ is not a product of fields. How can we interpret any of our pairings in this setting? To clarify this issue consider the case of an elliptic curve E over $\mathbb{Z}/p^2\mathbb{Z}$, not anomalous over $\mathbb{Z}/p\mathbb{Z}$. Then $\#E(\mathbb{Z}/p^2\mathbb{Z}) = p\#E(\mathbb{F}_p)$ and $E[p]$ is cyclic of order p. Define $\mu_p = \{1 + xp : 0 \leq x < p\} \subset (\mathbb{Z}/p^2\mathbb{Z})^*$. One can certainly define a bilinear pairing on $E[p]$ taking values in μ_p, but both the geometric theory and Miller's algorithm break down for curves over such rings: the entire p-torsion lies on a straight line.

As a result, we propose to map each $\mathbb{Z}/p^a\mathbb{Z}$ to its residue field $\mathbb{Z}/p\mathbb{Z}$, and hence to map $E(\mathbb{Z}/N\mathbb{Z})$ to a product of curves over finite prime fields (the E_i in Section 3). Our pairings are defined for such curves, and we can define the pairing over $\mathbb{Z}/N\mathbb{Z}$ to be any preimage of the gluing together of these pairings. (In the context of oracles, we insist that the choice of preimage is made in a deterministic way.) As in the squarefree case, this can be further generalised to curves over the rings $R_{N,f}$ considered in Section 3. This generalisation is essential if we wish to consider embedding degrees greater than 1. For the reduced Tate pairing, the second definition extends in the obvious way: g is replaced by the exponent of $(R_{N,f})^*$. For the first definition, a little care is required: in each local factor we power up by the exponent of the local multiplicative group divided by its gcd with r, then we glue together the local values by the Chinese Remainder Theorem. Again we comment that this generalisation of the first definition behaves well under reduction.

We can even abstract this further, and consider an elliptic curve over any finite commutative ring R. (This includes rings such as $R_{N,f}$.) Such a ring is a product of local rings, each having prime power order. Each local factor has a residue field (of prime power order), and we can map our curve over R to a curve over the product of these residue fields. Then, as above, we can define a pairing value in each residue field, glue these together, and finally take a preimage in R. Again both definitions of the reduced Tate pairing extend equally naturally.

8 Reduced Tate pairing oracles

What is the minimum amount of information that we must feed to an oracle for computing reduced Tate pairings over rings of the form $R = R_{N,f}$? Certainly we must supply the oracle with N and f, and an elliptic curve E defined over

the ring R, and two points P and Q on $E(R)$ whose pairing is to be returned. We might also supply the value of r (with P, but not necessarily Q, supposed to have order dividing r: something that the oracle can easily check), or we might leave it to the oracle to compute suitable r. (One pleasing feature of the reduced Tate pairing is that the pairing value coming from the minimal possible r is the same as that computed using a multiple of it: see Section 6 of [8].) If the curve has no points of order r over R, or if R does not contain an element of order r, then the pairing value is still defined, but may well be trivial.

We have therefore two flavours of oracle, depending on whether or not we know the value of r.

Oracle 1 *This oracle takes as its input $N \in \mathbb{N}$, $f \in \mathbb{Z}[X]$, E defined by equation (1) for some a_4, a_6 in $R = R_{N,f}$, points P and Q in $E(R)$, and $r \in \mathbb{N}$.*

The oracle performs the following checks, and returns 'fail' if any of them fail:

- $\gcd(N, 6) = 1$;
- $\gcd(N, 4a_4^3 + 27a_6^2) = 1$;
- *P and Q are in $E(R)$;*
- $rP = 0$.

If all of these consistency checks are passed, then the oracle returns the reduced Tate pairing of P and Q, with value in R.

Oracle 2 *This oracle takes as its input $N \in \mathbb{N}$, $f \in \mathbb{Z}[X]$, E defined by equation (1) for some a_4, a_6 in $R = R_{N,f}$, and points P and Q in $E(R)$.*

The oracle performs the following checks, and returns 'fail' if any of them fail:

- $\gcd(N, 6) = 1$;
- $\gcd(N, 4a_4^3 + 27a_6^2) = 1$;
- *P and Q are in $E(R)$.*

If all of these consistency checks are passed, then the oracle chooses (but does not reveal) r such that $rP = 0$, and returns the reduced Tate pairing of P and Q, with value in R.

If one can factor N then, by Miller's algorithm, one can implement either of these oracles in polynomial time (to find suitable r for the second, we can use fast point-counting techniques).

We now claim that such oracles can be used to build an integer factorisation algorithm.

Theorem 3. *Let $\mathcal{O}$ be a reduced-Tate-pairing oracle, either of the form Oracle 1 or of the form Oracle 2.*

Given a composite integer N, not a prime power, with $\gcd(N, 6) = 1$, we can use the oracle $\mathcal{O}$ to find a non-trivial factorisation of N in expected time $O(1)$ ring operations, using $O(1)$ oracle calls, on average.

Proof. We work with Definition 1 of the reduced Tate pairing in the proof, and remark afterwards how the proof adapts trivially if one prefers Definition 2.

Choose a random integer a in the range $1 < a < N$, and define

$$E_a : y^2z = x(x-z)(x-az) = x^3 - (a+1)x^2z + axz^2$$

which has discriminant $16a^2(a-1)^2$. (We could transform this equation into Weierstrass form, as in (1), if desired.) This is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ as long as $\gcd(N, 2a(a-1)) = 1$. We take $r = 2$ and note that the points $P = (0:0:1), Q = (1:0:1)$ and $R = (a:0:1)$ all have order 2.

One can compute the Tate pairing over $\mathbb{Q}$ of P with itself. The function $F = x$ satisfies $(F) = 2(P) - 2(0)$. If Q is taken to be the auxiliary point then the Tate pairing of P and $P + 2E$ is

$$\langle P, P\rangle_2 = F(P+Q)/F(Q) = x(R)/x(Q) = a/1 = a.$$

If another auxiliary point $(u:v:1)$ is used then

$$P + (u:v:1) = (a/u : -av/u^2 : 1)$$

and so the pairing value is a/u^2.

Calling the oracle $\mathcal{O}$ (with arguments N, $f = 1$, $P = Q = (0:0:1)$, and $r = 2$ (if needed)) performs exactly the operation of the oracle $\mathcal{O}(N, 2, a)$ in Section 6. Hence we can use the reduced Tate pairing oracle $\mathcal{O}$ to find a non-trivial factorisation of N in $O(1)$ ring operations, as in Lemma 1 (with $r = 2$). □

We remark that if instead the reduced Tate pairing were defined by Definition 2, then the reduction to integer factorisation is just as simple. If the power of 2 dividing $p_i - 1$ is the same for each prime p_i dividing N, then the identical argument works. If not, then the reduced pairing is guaranteed to be trivial modulo at least one but not all of the p_i, and a similar argument goes through, analogous to Lemma 4.

The idea of the proof can be generalised to other small values of r, starting from a curve over $\mathbb{Q}$ (or a low-degree number field) with an r-torsion point.

Inspired by the quadratic residuosity observations in section 2, we note that the situation is still more favourable here, at least if we work with our preferred definition of the reduced Tate pairing.

Theorem 4. *Let N be an odd, composite integer, and let $\mathcal{O}$ be an oracle that tells us whether or not the reduced Tate pairing (as in Definition 1) of two points on an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ is trivial.*

Given $a \in (\mathbb{Z}/N\mathbb{Z})^*$ satisfying $\left(\frac{a}{N}\right) = 1$, we can use the oracle $\mathcal{O}$ to determine whether or not a is a square in $(\mathbb{Z}/N\mathbb{Z})^*$ with a single call to the oracle $\mathcal{O}$.

Proof. As above, we take the curve

$$E_a : y^2z = x(x-z)(x-az) = x^3 - (a+1)x^2z + axz^2\,,$$

and ask the oracle $\mathcal{O}$ whether or not the reduced Tate pairing of $P = (0:0:1)$ with itself is trivial. The answer is 'yes' precisely when a is a square in $(\mathbb{Z}/N\mathbb{Z})^*$. □

9 Acknowledgments

The authors gratefully acknowledge the insight of Jorge Villar, who pointed out some inadequacies in an early version of this paper, and the comments of the referees.

References

1. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, in J. Kilian (ed.), CRYPTO 2001, Springer LNCS 2139 (2001) 213–229.
2. D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing, *J. Crypt*, **17**, No. 4 (2004) 297–319.
3. J.W.S. Cassels, *Lectures on Elliptic Curves*, LMS Student Texts **24**, Cambridge (1991).
4. N. Demytko, A new elliptic curve based analogue of RSA, in T. Helleseth (ed.), EUROCRYPT 1993, Springer LNCS 765 (1994) 40–49.
5. G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.*, **52** (1994) 865–874.
6. G. Frey, M. Müller and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inf. Th.*, **45** (1999) 1717–1719.
7. S.D. Galbraith, Elliptic curve Paillier schemes, *J. Crypt.*, **15**, No. 2 (2002) 129–138.
8. S.D. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing, in C. Fieker and D.R. Kohel (eds.), ANTS V, Springer LNCS 2369 (2002) 324–337.
9. M. Girault, An Identity-Based Identification Scheme Based on Discrete Logarithms Modulo a Composite Number, in I.B. Damgard (ed.), EUROCRYPT 1990, Springer LNCS 473 (1991) 481–486.
10. A. Joux, A One Round Protocol for Tripartite Diffie-Hellman, in W. Bosma (ed.), ANTS IV, Springer LNCS 1838 (2000) 385–394.
11. N. Kunihiro and K. Koyama, Equivalence of counting the number of points on elliptic curve over the ring $\mathbb{Z}_n$ and factoring n, in K. Nyberg (ed.), EUROCRYPT 1998, Springer LNCS 1403 (1998) 47–58.
12. K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone, New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, in J. Feigenbaum (ed.), CRYPTO 1991, Springer LNCS 576 (1992) 252–266.
13. H.W. Lenstra Jr., Factoring integers with elliptic curves, *Annals of Mathematics*, **126** (1987) 649–673.
14. H.W. Lenstra Jr., Elliptic curves and number theoretic algorithms, *Proc. International Congr. Math.*, Berkeley 1986, AMS (1988) 99–120.
15. C.H. Lim and P.J. Lee, Security and performance of server-aided RSA computation protocols, in D. Coppersmith (ed.), CRYPTO 1995, Springer LNCS 963 (1995) 70–83.
16. W. Mao, Verifiable partial sharing of integer factors, in S. Tavares and H. Meijer (eds.), SAC 1998, Springer LNCS 1556 (1998) 94–105.
17. S. Martin, P. Morillo and J.L. Villar, Computing the order of points on an elliptic curve modulo N is as difficult as factoring N, *Applied Math. Letters*, **14** (2001) 341–346.
18. J.F. McKee, Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field, *J. London Math. Soc.* (2), **59** (1999) 448–460.
19. J.F. McKee and R.G.E. Pinch, Old and new deterministic factoring algorithms, in H. Cohen (ed.), ANTS II, Springer LNCS 1122 (1996) 217–224.

20. J.F. McKee and R.G.E. Pinch, Further attacks on server-aided RSA cryptosystems, unpublished manuscript (1998).
21. B. Meyer and V. Mueller, A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring, in U.M. Maurer (ed.), EUROCRYPT 1996, Springer LNCS 1070 (1996) 49–59.
22. V.S. Miller, Short programs for functions on curves, unpublished manuscript (1986).
23. V.S. Miller, The Weil pairing, and its efficient calculation, *J. Crypt.*, **17**, No. 4 (2004) 235–261.
24. T. Okamoto and S. Uchiyama, Security of an identity-based cryptosystem and the related reductions, in K. Nyberg (ed.), EUROCRYPT 1998, Springer LNCS 1403 (1998) 546–560.
25. J.M. Pollard, A Monte Carlo method for factorisation, *BIT*, **15** (1975) 331–334.
26. J.M. Pollard, Monte Carlo methods for index computations (mod p), *Math. Comp.*, **32** (1978) 918–924.
27. M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, Technical report TR-212, MIT Laboratory for Computer Science (1979).
28. M. Scott and P.S.L.M. Barreto, Compressed pairings, in M. K. Franklin (ed.), CRYPTO 2004, Springer LNCS 3152 (2004) 140–156.
29. D. Shanks, Class number, a theory of factorisation and genera, in D.J. Lewis (ed.), Number theory institute 1969, Proceedings of symposia in pure mathematics, vol. 20, Providence RI, AMS (1971) 415–440.
30. J.W.M. Turk, Fast arithmetic operations on numbers and polynomials, in H.W. Lenstra Jr. and R. Tijdeman (eds.), Computational methods in number theory, Part 1, Mathematical Centre Tracts 154, Amsterdam (1984).
31. S.A. Vanstone and R.J. Zuccherato, Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$, *IEEE Trans. Inform. Theory*, **43**, No.4 (1997) 1231–1237.