Efficient Multiplication on Certain Nonsupersingular Elliptic Curves

Willi Meier [1)] Othmar Staffelbach [2)]

[1)] HTL Brugg-Windisch
CH-5200 Windisch, Switzerland

[2)] Gretag Data Systems AG
CH-8105 Regensdorf, Switzerland

Abstract

Elliptic curves defined over finite fields have been proposed for Diffie-Hellman type crypto systems. Koblitz has suggested to use "anomalous" elliptic curves in characteristic 2, as these are nonsupersingular and allow for efficient multiplication of points by an integer.

For anomalous curves E defined over $\mathbf{F}_2$ and regarded as curves over the extension field $\mathbf{F}_{2^n}$, a new algorithm for computing multiples of arbitrary points on E is developed. The algorithm is shown to be three times faster than double and add, is easy to implement and does not rely on precomputation or additional memory. The algorithm is used to generate efficient one-way permutations involving pairs of twisted elliptic curves by extending a construction of Kaliski to finite fields of characteristic 2.

1 Introduction

Elliptic curves defined over finite fields have been proposed for Diffie-Hellman type crypto systems [7,4] as well as for implementation of one-way permutations [2]. In particular, in [3] Koblitz has described the class of "anomalous" elliptic curves which in characteristic 2 have the following useful properties

1. They are nonsupersingular, so that one cannot use the Menezes-Okamoto-Vanstone reduction [6] of discrete logarithms from elliptic curves to finite fields.

2. Multiplication of points by an integer m can be carried out almost as efficiently as in the case of supersingular curves.

According to [3] an elliptic curve E defined over the field $\mathbf{F}_q$ is called anomalous if the trace of the Frobenius map $((x, y) \mapsto (x^q, y^q))$ is equal to 1. Equivalently, an elliptic curve over $\mathbf{F}_q$ is anomalous if and only if the number of $\mathbf{F}_q$-points is equal

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 333-344, 1993.
© Springer-Verlag Berlin Heidelberg 1993

to q. As in [3] we will concentrate on curves in characteristic 2, and in particular on the anomalous curve

$$E : y^2 + xy = x^3 + x^2 + 1 \tag{1}$$

defined over $\mathbf{F}_2$. We will also consider its twist $\tilde{E}$ over $\mathbf{F}_2$, which is given by the equation $y^2 + xy = x^3 + 1$. Subsequently these curves will be considered over the extension fields $\mathbf{F}_{2^n}$. Hereby let E_n denote the $\mathbf{F}_{2^n}$-points of the curve E, and $\tilde{E}_n$ its twist over $\mathbf{F}_{2^n}$.

In applications, e.g., in a Diffie-Hellman key exchange, multiples mP of points P on the curve E_n have to be computed. In standard algorithms for multiplication, e.g, by double and add, this is reduced to a number of additions of points on E_n. Since these additions consume most of the computation time, it is desirable to have algorithms which need fewer additions on E_n. In [3] it is suggested to express multiplication by m as linear combinations of powers of the Frobenius map ϕ, as these can be computed by iterated squaring in $\mathbf{F}_{2^n}$ which, in a normal basis representation, is easily accomplished by shift operations. In [3] expansions of the form

$$m = \sum_j c_j \phi^j \tag{2}$$

are considered with $c_j \in \{0, \pm 1\}$. With this representation of m the computation of mP can be reduced to $l - 1$ additions where l is the number of nonzero terms in (2). Therefore it is desirable to have short expressions (2). The expansions given in [3] in the average have twice the length of the binary expansion of m.

In this paper we elaborate constructions of short expansions (2). In particular, in Section 2 we prove that there always exists an expansion $m = \sum_{j=0}^{n-1} c_j \phi^j$ of length n, where n is the degree of the extension field (Theorem 1). The proof of Theorem 1 leads to an efficient algorithm which produces expansions where half of the coefficients c_j are expected to be zero (Corollary 4).

Our construction exploits the fact that the endomorphism ring $\mathrm{End}(E)$ of the curve E is related to the ring $\mathbf{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$, where $\alpha = (1 + \sqrt{-7})/2$. In particular we will reduce the problem of finding ϕ-expansions in $\mathrm{End}(E)$ to finding α-expansions in $\mathbf{Z}[\alpha]$, where we make specific use of the rich algebraic structure of the ring $\mathbf{Z}[\alpha]$. The computational complexity of the reduction algorithm is of magnitude of a n-bit integer multiplication.

Since execution of ϕ^j is obtained almost for free, the ϕ-expansion of m allows to compute mP for an arbitrary point P on E_n with $n/2$ additions in the average. As the computation of the ϕ-expansion is negligible compared with a full multiplication by m on the curve, this results in an improvement by a factor 3 compared to double and add without using precomputation or additional memory. At this point we note that other methods have been proposed for accelerating this operation (see e.g., [1]). However these methods only apply if the point P is assumed to be fixed. Furthermore they need precomputation with this predefined point P (and additional memory). Observe for example that P cannot be assumed to be fixed in the second step of a Diffie-Hellman key exchange protocol.

Our results also apply to generate efficient one-way permutations based on elliptic curves. In [2] Kaliski has proposed a construction of one-way permutations involving

pairs of twisted elliptic curves over $\mathbf{F}_p$ for large prime numbers p. It is easy to generalize the treatment in [2] to any extension field $\mathbf{F}_{p^n}$ of $\mathbf{F}_p$. In Section 3 we apply the construction to extension fields $\mathbf{F}_{2^n}$ in characteristic 2. The treatment in characteristic 2 differs from the treatment in odd characteristic. However the construction in characteristic 2 appears to be particularly attractive, as arithmetic can be carried out efficiently. On certain curves, arithmetic can be accelerated by using the ϕ-expansion of multiplication by m. Restriction to curves with short ϕ-expansion leaves enough freedom to find examples of curves with good cryptographic properties.

2 Frobenius Expansion of Multiplication by m

On an anomalous curve over $\mathbf{F}_q$, the Frobenius map ϕ satisfies the characteristic equation $T^2 - T + q = 0$. We will also consider the twist $\tilde{E}$ of E, whose Frobenius satisfies $T^2 + T + q = 0$. The number of $\mathbf{F}_q$-points on $\tilde{E}$ is $q + 2$. The "n-twist" $\tilde{E}_n$ is the twist of E regarded as curve over the extension field $\mathbf{F}_{q^n}$. Using the Weil conjecture (see [8, p. 136]), the number N_n of $\mathbf{F}_{q^n}$-points can be computed as

$$N_n = |\alpha^n - 1|^2 = |\beta^n - 1|^2 = 1 + q^n - \alpha^n - \beta^n, \tag{3}$$

where α and β in $\mathbf{C}$ are the roots of the characteristic equation $T^2 - T + q = 0$. The number $\tilde{N}_n$ of points on the twist $\tilde{E}_n$ is given by $\tilde{N}_n = |\alpha^n + 1|^2 = 1 + q^n + \alpha^n + \beta^n$. Equivalently, N_n and $\tilde{N}_n$ can be computed as $N_n = q^n + 1 - a_n$ and $\tilde{N}_n = q^n + 1 + a_n$, where $a_n = \alpha^n + \beta^n$ for $n \geq 2$ satisfies the recursion $a_n = a_{n-1} - q a_{n-2}$ with the initial values $a_0 = 2$ and $a_1 = 1$.

We now will concentrate on anomalous curves in characteristic 2, and in particular on the anomalous curve $E : y^2 + xy = x^3 + x^2 + 1$ defined over $\mathbf{F}_2$. Its twist over $\mathbf{F}_2$ is given by $\tilde{E} : y^2 + xy = x^3 + 1$. Let E_n denote the curve E regarded over the extension field $\mathbf{F}_{2^n}$, and $\tilde{E}_n$ its twist over $\mathbf{F}_{2^n}$.

Our aim in this section is to express multiplication by m as short linear combinations of powers of the Frobenius map ϕ, as this will lead to an efficient computation of multiples mP of arbitrary points on E_n. In [3] expansions of the form

$$m = \sum_j c_j \phi^j \tag{4}$$

are considered with $c_j \in \{0, \pm 1\}$. The expansions given in [3] in the average have twice the length of the binary expansion of m. On the other hand, from [5, p. 149] one concludes that there must be shorter expansions of the form

$$m = \sum_{j=0}^{n-1} a_j \phi^j, \tag{5}$$

possibly with larger coefficients, however. From [5] one can merely deduce that $|a_j| \leq 7$.

In the following theorem we show that one can construct expansions which simultaneously satisfy the conditions of (4) and (5).

Theorem 1 *For the anomalous curve $E : y^2 + xy = x^3 + x^2 + 1$ defined over $\mathbf{F}_2$, let E_n be the curve regarded over the extension field $\mathbf{F}_{2^n}$. Then on E_n multiplication by an integer m can be expressed as*

$$m = \sum_{j=0}^{n-1} c_j \phi^j, \tag{6}$$

with $c_j \in \{0, \pm 1\}$.

This theorem also holds for $\tilde{E}_n$. The proof proceeds in several steps. First observe that the Frobenius map satisfies the equation $\phi^2 - \phi + 2 = 0$, and that there is a natural homomorphism from the ring $\mathbf{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$ to the endomorphism ring $\mathrm{End}(E)$ of E which maps $\alpha = (1+\sqrt{-7})/2$ to ϕ. Thus, if we have an expansion $m = \sum_j c_j \alpha^j$ in $\mathbf{Z}[\alpha]$, we immediately get a corresponding expansion $m = \sum_j c_j \phi^j$ in $\mathrm{End}(E)$. This means that $mP = \sum_j c_j \phi^j(P)$ for every point P on E_n. For finding such an expansion in $\mathbf{Z}[\alpha]$ we will make use of the algebraic structure of the ring $\mathbf{Z}[\alpha]$. Note that $\mathbf{Z}[\alpha]$ is an Euclidean domain with respect to the norm $N(a + b\alpha) = |a + b\alpha|^2 = (a + b\alpha)(a + b\overline{\alpha}) = a^2 + ab + 2b^2, a, b \in \mathbf{Z}$. For the proof of the theorem we will make use of the following stronger property.

Lemma 2 *For any $s, t \in \mathbf{Z}[\alpha]$, $t \neq 0$, there exist $q, r \in \mathbf{Z}[\alpha]$ such that $s = qt + r$ with*

$$N(r) \leq \frac{4}{7} N(t). \tag{7}$$

Proof. The elements of the ring $\mathbf{Z}[\alpha]$ form a lattice in $\mathbf{C}$, and the whole of $\mathbf{C}$ can be covered by triangles whose vertices are in $\mathbf{Z}[\alpha]$, as depicted in Figure 1. Consider the

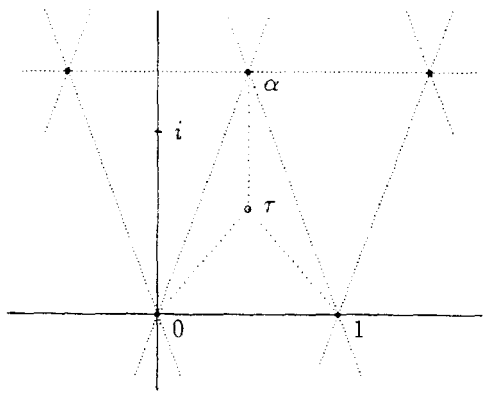

Figure 1: The lattice $\mathbf{Z}[\alpha]$.

triangle with vertices 0, 1 and α. The point $\tau = 1/2 + (3/(2\sqrt{7}))\, i$ is the center of the circumscribed circle of the triangle, as is easily verified by computing the distance of

τ to each vertex, that is $|\tau - 0| = |\tau - 1| = |\tau - \alpha| = 2/\sqrt{7}$. It follows that any other point in the triangle has distance less than $2/\sqrt{7}$ to some vertex. Since any point $z \in \mathbf{C}$ lies in some triangle, we conclude that for any complex number $z \in \mathbf{C}$ there is an element $u \in \mathbf{Z}[\alpha]$ with $N(z-u) \leq (2/\sqrt{7})^2 = 4/7$.

Now let $s, t \in \mathbf{Z}[\alpha]$ with $t \neq 0$. Consider the quotient $v = s/t$ computed in the quotient field of $\mathbf{Z}[\alpha]$, i.e., in the field $\mathbf{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbf{Q}\} \subset \mathbf{C}$. Then, as discussed above, there is an element $q \in \mathbf{Z}[\alpha]$ with $N(v-q) \leq 4/7$, and $r = s - qt = t(v-q)$ has norm $N(r) = N(v-q)N(t) \leq (4/7)N(t)$, which implies that $q, r \in \mathbf{Z}[\alpha]$ have the properties as stated in the lemma. □

Lemma 3 *For any $s \in \mathbf{Z}[\alpha]$ with norm $N(s) < 2^n$, $n \in \mathbf{N}$, there is an expansion*

$$s = \sum_{j=0}^{n-1} c_j \alpha^j \tag{8}$$

of length n with $c_j \in \{0, \pm 1\}$.

Proof. The proof is by induction on n. For $n = 1, 2$, consider the elements in $\mathbf{Z}[\alpha]$ with norm less than 4. These are the element 0 with norm 0, the elements ± 1 with norm 1 and the elements $\pm\alpha, \pm(1-\alpha)$ with norm 2. For these elements the statement of the lemma holds as is seen by direct inspection.

Now consider $s \in \mathbf{Z}[\alpha]$ with $N(s) < 2^n, n > 2$. Since $\mathbf{Z}[\alpha]$ is an Euclidean domain, s can be expressed as

$$s = s'\alpha + c \tag{9}$$

with $N(c) < N(\alpha) = 2$, i.e., with $c \in \{0, \pm 1\}$. The idea is to reduce the problem of finding an expansion for s to the problem of finding an expansion for s'. If $c = 0$, i.e., if α divides s, the reduction (9) is unique. Otherwise, as α divides 2, there is always a reduction with $c = 1$ and another reduction with $c = -1$. If the reduction could be done such that $N(s') \leq N(s)/2 < 2^{n-1}$, the proof would easily be completed by induction. There are situations however, where there is no reduction with $N(s') \leq N(s)/2$, as we shall see below. We will distinguish between the following three cases:

1. *Non-critical case:* There is a reduction (9) with $N(s') < N(s)/2$.
2. *Semi-critical case:* There is a reduction (9) with $N(s') = N(s)/2$.
3. *Critical case:* There are only reductions (9) with $N(s') > N(s)/2$.

If α divides s, we have the reduction $s = s'\alpha$ with $c = 0$ and $N(s') = N(s)/2$, i.e., s is semi-critical. If α does not divide s, α is a divisor of both, $s - 1$ and $s + 1$. In this case the type of the reduction turns out to depend on the absolute value of the real part $\Re(s)$ of s:

1. Non-critical case: $|\Re(s)| \geq 1$. Assume for example that $\Re(s) \geq 1$, as illustrated for $s = s_1$ in Figure 2. Then $N(s-1) < N(s)$, and we have the reduction $s = s'\alpha + 1$ with $N(s') = N(s-1)/N(\alpha) < N(s)/2$. Similarly, if $\Re(s) \leq -1$, we have $s = s'\alpha - 1$ with $N(s') < N(s)/2$.

2. Semi-critical case: $|\Re(s)| = 1/2$. Assume for example that $\Re(s) = 1/2$, as illustrated for $s = s_2$ in Figure 2. Then $N(s-1) = N(s)$, and we have the reduction $s = s'\alpha + 1$ with $N(s') = N(s-1)/N(\alpha) = N(s)/2$. Similarly, if $\Re(s) = -1/2$, we have $s = s'\alpha - 1$ with $N(s') = N(s)/2$.

3. Critical case: $\Re(s) = 0$. This is illustrated for $s = s_3$ in Figure 2. Then, by Pythagoras' theorem, $N(s-1) = N(s+1) = N(s) + 1$, and we have the reductions $s = s'\alpha + 1$ and $s = s''\alpha - 1$ with

$$N(s') = N(s'') = \frac{N(s)+1}{2} \tag{10}$$

Since $s'' - s' = 2/\alpha = 1 - \alpha$, either s' or s'' is not divisible by α. Assume that s' is not divisible by α. We claim that s' has a non-critical reduction. For this it suffices to show that $|\Re(s')| \geq 1$.

Since $\Re(s) = 0$, s must be of the form $s = a\sqrt{-7}$ for some odd integer $a \in \mathbf{Z}$. Then s' can be computed in $\mathbf{Q}(\alpha)$ as

$$s' = (s-1)\alpha^{-1} = (a\sqrt{-7} - 1)\frac{1}{4}(1 - \sqrt{-7}) = \frac{7a-1}{4} + \frac{a+1}{4}\sqrt{-7}.$$

It follows that $|\Re(s')| \geq 3/2$. Hence s' is non-critical. Similarly, s'' is non-critical if α does not divide s''.

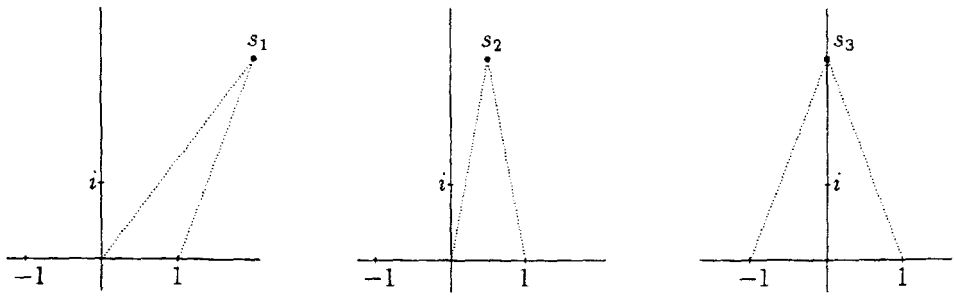

Figure 2:

Now the proof of the lemma is easily accomplished. In case that s has a non-critical or semi-critical reduction $s = s'\alpha + c$, we have $N(s') \leq N(s)/2 < 2^{n-1}$. By induction hypothesis, s' has an expansion in α of length $n-1$, which yields an expansion of s in α of length n.

In case that s has a critical reduction $s = s'\alpha + c$, we have according to (10), $N(s') = (N(s)+1)/2 \leq 2^{n-1}$. Since the inequality $N(s') \leq 2^{n-1}$ does not hold strictly, we cannot apply the induction hypothesis to s'. However, as discussed above, the reduction can be done such that s' has a non-critical reduction $s' = s''\alpha + c'$, i.e., $N(s'') < N(s')/2 \leq 2^{n-2}$. Thus $s = s''\alpha^2 + c'\alpha + c$, and by induction hypothesis, s''

has an expansion in α of length $n-2$, which yields an expansion of s in α of length n. This completes the proof of the lemma. □

Now we are in position to prove Theorem 1. As the curve E_n is regarded over the extension field $\mathbf{F}_{2^n}$, the Frobenius map satisfies the equation $\phi^n = 1$. It follows that for any two α-expansions which are congruent modulo $\alpha^n - 1$ the corresponding ϕ-expansions yield the same endomorphism on E_n. Therefore we compute the α-expansion of the remainder m' of the division of m by $\alpha^n - 1$,

$$m = q(\alpha^n - 1) + m', \tag{11}$$

where, according to Lemma 2, $N(m') \leq (4/7)N(\alpha^n - 1)$. To obtain a bound on $N(m')$ we compute (see formula (3))

$$N(\alpha^n - 1) = (\alpha^n - 1)(\beta^n - 1) = (\alpha\beta)^n - (\alpha^n + \beta^n) + 1 = 2^n + 1 - (\alpha^n + \beta^n) = N_n. \tag{12}$$

By Hasse's theorem (see [8, p.131]), $N_n \leq f(n) = 2^n + 1 + 2^{n/2+1}$, and for $n \geq 4$, $(4/7)f(n) < 2^n$, as $g(n) = 2^n - (4/7)f(n)$ is strictly increasing for $n \geq 1$ and strictly positive for $n = 4$. Hence for $n \geq 4$, $N(m') < 2^n$ and the theorem follows from Lemma 3. For $n \leq 3$ the statement of the theorem can be verified directly. □

Note that an arbitrary element $s = a + b\alpha$ in $\mathbf{Z}[\alpha]$ is divisible by α if and only if a is even. Hence with probability $1/2$ this element has a reduction of the form $s = s'\alpha$, i.e., with $c = 0$. Continuing the reduction, it is to be expected that the intermediate results s' also have this property. This would imply that half of the coefficients c_j in (8) can be expected to be zero. This has been confirmed experimentally.

Corollary 4 (Experimental result) *In the expansion* $m = \sum_{j=0}^{n-1} c_j \phi^j$ *half of the coefficients* c_j *are expected to be zero.*

It is easy to compute the α-expansion of an arbitrary element $s = a + b\alpha \in \mathbf{Z}[\alpha]$. From the proof of Lemma 3 one can derive the following simple and efficient procedure which outputs c_j in ascending order for j.

```
While a ≠ 0 or b ≠ 0 do begin
    if a is even then
        c := 0;
    else begin
        if 2a + b ≠ 0 then c := sgn(2a + b);
        if 2a + b = 0 then begin
            if a ≡ 1 (mod 4) then c := −1;
            if a ≡ 3 (mod 4) then c := 1;
        end;
    end;
    x := (a − c)/2;   a := x + b;   b := −x;
    output(c);
end.
```

The problem of efficiently finding short ϕ-expansions of multplication by an arbitrary m was addressed by Koblitz in [3]. In the above procedure, the amount of work to perform the division (11) is roughly of the same magnitude as to perform the reduction. This is of magnitude of a n-bit integer multiplication, and is negligible in comparison with a full multiplication by m on the elliptic curve.

As execution of ϕ^j is obtained almost for free, according to Corollary 4, multiplication by m can be carried out with $n/2$ additions in the average. This results in an improvement by a factor 3 compared to double and add without using precomputation or additional memory.

The results of Theorem 1 and Corollary 4 may also be applied to the key exchange procedure suggested by H. Lenstra as mentioned in [3, p.285]. In this suggestion one chooses expansions $m = \sum_{j=0}^{n-1} c_j \phi^j$ where only a certain maximum number of coefficients c_j are allowed to be nonzero. However it is unclear which multiples are obtained when applying this restriction. Furthermore certain multiples could occur more than once which would result in a non uniform probability distribution of the chosen values of m, or in a non uniform distribution of the keys. Theorem 1 allows to obtain every multiple with the same probability by choosing m first and then making the reduction.

3 One-Way Permutations on Elliptic Curves in Characteristic 2

In [2] elliptic curves have been suggested as a tool for generating one-way permutations. Two constructions have been proposed in [2], one involving single elliptic curves and the other one involving pairs of twisted elliptic curves. Both constructions deal with curves over $\mathbf{F}_p$ for large prime numbers p. As already observed in [2], the elliptic curves used in the first construction are supersingular, so that the Menezes-Okamoto-Vanstone reduction [6] can be applied. The second construction applies to arbitrary elliptic curves over $\mathbf{F}_p$ for any odd prime number $p > 3$. It is easy to generalize the treatment in [2] to any extension field $\mathbf{F}_{p^n}$ of $\mathbf{F}_p$.

In this section we apply the second construction to extension fields $\mathbf{F}_{2^n}$ in characteristic 2. The treatment in characteristic 2 differs from the treatment in odd characteristic. However the construction in characteristic 2 appears to be particularly attractive for the following reasons.

1. Arithmetic in characteristic 2 can be carried out efficiently.
2. On certain curves, arithmetic can be accelerated by using the ϕ-expansion of multiplication by m.
3. Even restriction to anomalous curves leaves enough freedom to find curves with good cryptographic properties.

In the following all curves are considered to be defined over fields with characteristic 2. Recall that an elliptic curve in characteristic 2 is nonsupersingular if and only if

the j-invariant is nonzero (see [8, p. 145]). The normal form of an elliptic curve E with $j(E) \neq 0$ is given by

$$y^2 + xy = x^3 + a_2x^2 + a_6, \tag{13}$$

where $a_6 \neq 0$. If a_2, a_6 are in $\mathbf{F}_{2^n}$, the curve is defined over $\mathbf{F}_{2^n}$. The twist $\tilde{E}$ of E, up to isomorphism, is given by

$$y^2 + xy = x^3 + (a_2 + D)x^2 + a_6, \tag{14}$$

where $D \in \mathbf{F}_{2^n}$ is such that the polynomial $t^2 + t + D$ is irreducible over $\mathbf{F}_{2^n}$. Observe that E and $\tilde{E}$ are non-isomorphic over $\mathbf{F}_{2^n}$ but are isomorphic over $\mathbf{F}_{2^{n+1}}$. Now we prove the analogue of Lemma 4.1 in [2].

Lemma 5 *Every nonzero $x \in \mathbf{F}_{2^n}$ appears either as x-coordinate of exactly two points on E or as x-coordinate of exactly two points on $\tilde{E}$. The elliptic curve E together with its twist $\tilde{E}$ have order $2(2^n + 1)$, i.e., $\#E + \#\tilde{E} = 2(2^n + 1)$.*

Proof. For a fixed $x \neq 0$ the equation in y for (x, y) to be on E can be written as

$$t^2 + t + c = 0, \tag{15}$$

with $t = y/x$ and where $c = (x^3 + a_2x^2 + a_6)/x^2$ is a constant. Similarly, with the same notation, the equation in y for (x, y) to be on $\tilde{E}$ is

$$t^2 + t + (c + D) = 0. \tag{16}$$

The equation $t^2 + t + c = 0$ has a solution if and only if c is in the image of the mapping $Q : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}, Q(t) = t^2 + t$. Since Q is a homomorphism of the additive group $\mathbf{F}_{2^n}$, with kernel $\mathbf{F}_2$, the image $\operatorname{im} Q$ is a subgroup of index 2 in $\mathbf{F}_{2^n}$. By assumption $t^2 + t + D$ is irreducible over $\mathbf{F}_{2^n}$, hence $D \notin \operatorname{im} Q$. As a consequence exactly one of the two elements c and $c + D$ is in $\operatorname{im} Q$. This implies that exactly one of the equations (15) and (16) has (two) solutions. Thus we conclude that every nonzero x appears either as x-coordinate of exactly two points on E or as x-coordinate of exactly two points on $\tilde{E}$, which implies the first part of the lemma.

For $x = 0$ we get the equation $y^2 = a_6$ for both curves. This equation always has exactly one solution, as squaring in F_{2^n} is a bijection. The latter holds as 2 is relatively prime to $|\mathbf{F}_{2^n}^*| = 2^n - 1$. Counting the points on E and $\tilde{E}$ we get $2(2^n - 1)$ points with $x \neq 0$, two points with $x = 0$ and the two points at infinity. This implies that $\#E + \#\tilde{E} = 2(2^n + 1)$ (which also follows from the Weil conjecture (3)). □

Our aim is to identify the elements of E and $\tilde{E}$ with certain integers. For a given representation of the elements of $\mathbf{F}_{2^n}$ as residues modulo a fixed irreducible polynomial, we first identify the elements of $\mathbf{F}_{2^n}$ with the integers $0, 1, \ldots, 2^n - 1$ as follows: The polynomial $f(t) = c_{n-1}t^{n-1} + \ldots + c_1t + c_0 \in \mathbf{F}_2[t]$ considered as element of $\mathbf{F}_{2^n}$ is identified with the integer $c_{n-1}2^{n-1} + \ldots + c_12 + c_0$. This bijection defines an ordering of $\mathbf{F}_{2^n}$. This ordering is in no way compatible with the algebraic structure of the field, but we can use it to construct a map ℓ from $E \cup \tilde{E}$ to the integers.

First we define ℓ on E. For $x \neq 0$ suppose that $(x,y) \in E$. Then $(x, x+y)$ is the other point on E with the same x-coordinate. The idea in the definition of ℓ is to map the point with the smaller y-coordinate to the set $1, \ldots, 2^n-1$ and the point with the larger y-coordinate to the set $2^n+2, \ldots, 2^{n+1}$.

$$\begin{aligned}
\ell(x,y) &= 0 && \text{if } x = 0 \text{ and } y = \sqrt{a_6} && (17)\\
\ell(x,y) &= x && \text{if } x \neq 0 \text{ and } y < x+y && (18)\\
\ell(x,y) &= x + 2^n + 1 && \text{if } x \neq 0 \text{ and } y > x+y && (19)\\
\ell(\infty) &= 2^n && && (20)
\end{aligned}$$

The definition of ℓ on $\tilde{E}$ is similar.

$$\begin{aligned}
\ell(x,y) &= 2^n + 1 && \text{if } x = 0 \text{ and } y = \sqrt{a_6} && (21)\\
\ell(x,y) &= x && \text{if } x \neq 0 \text{ and } y < x+y && (22)\\
\ell(x,y) &= x + 2^n + 1 && \text{if } x \neq 0 \text{ and } y > x+y && (23)\\
\ell(\infty) &= 2^{n+1} + 1 && && (24)
\end{aligned}$$

Theorem 6 *Let $E : y^2 + xy = x^3 + a_2x^2 + a_6$ be a nonsupersingular elliptic curve, and $\tilde{E} : y^2 + xy = x^3 + (a_2 + D)x^2 + a_6$ its twist over $\mathbf{F}_{2^n}$. Then the map ℓ as defined in (17) - (24) is a bijection from $E \cup \tilde{E}$ to the set of numbers $\{0, 1, \ldots, 2^{n+1}+1\}$.*

Proof. According to Lemma 5 the set of possible nonzero x-coordinates of points on E and on $\tilde{E}$ are disjoint. Therefore ℓ, as defined in (17) - (24), is injective. Hence ℓ is bijective, as by Lemma 5 the two sets have the same cardinality. □

We now assume that both curves E and $\tilde{E}$ are cyclic with generators $G \in E$ and $\tilde{G} \in \tilde{E}$. Let N denote the order of E. Then we define a map $f : \{0, \ldots, 2^{n+1}+1\} \to \{0, \ldots, 2^{n+1}+1\}$, as in [2] by

$$\begin{aligned}
f(m) &= \ell(mG) \quad \text{if} \quad 0 \leq m < N && (25)\\
f(m) &= \ell(m\tilde{G}) \quad \text{if} \quad N \leq m < 2^{n+1} + 2 && (26)
\end{aligned}$$

As a consequence of Theorem 6 we obtain the following

Corollary 7 *Let $E : y^2 + xy = x^3 + a_2x^2 + a_6$ be a nonsupersingular elliptic curve, and $\tilde{E} : y^2 + xy = x^3 + (a_2 + D)x^2 + a_6$ its twist over $\mathbf{F}_{2^n}$. If both curves E and $\tilde{E}$ are cyclic, then the function f as defined in (25) and (26) is a permutation of the set $\{0, \ldots, 2^{n+1}+1\}$.*

As observed in [2], inverting the permutation f is equivalent to solving the discrete logarithm problem on the elliptic curves.

Our aim is to find practical examples where both curves E and $\tilde{E}$ are cyclic. At the same time the order of each curve should have at least one large prime divisor such that computation of discrete logarithms is supposed to be hard. A finite abelian group is cyclic if and only if the p-primary component of the group is cyclic for each prime p dividing the order of the group. For the p-primary component for $p = 2$ we have

Proposition 8 *For a nonsupersingular elliptic curve in characteristic 2 the 2-primary component is always cyclic.*

Proof. Let $P_0 = (x_0, y_0) \in E$ be a point of order 2, i.e. $2P_0 = 0$, or $P_0 = -P_0$. For $j(E) \neq 0$ the curve E has the normal form $y^2 + xy = x^3 + a_2x^2 + a_6$, and the negative of a point $P = (x, y)$ is computed as $-P = (x, -y - x)$ (see [8, p. 58]). This implies that $y_0 = -y_0 - x_0$, hence $x_0 = -2y_0 = 0$ and $y_0 = \sqrt{a_6}$, i.e., there is only one point of order 2. □

In order to guarantee that the p-primary component is cyclic for odd primes p we are looking for curves whose order is not divisible by p^2. For examples we concentrate on the anomalous curve $E : y^2 + xy = x^3 + x^2 + 1$ defined over $\mathbf{F}_2$ as discussed in Section 2. Thus denote by N_n the number of $\mathbf{F}_{2^n}$-points on E and by $\tilde{N}_n$ the number of $\mathbf{F}_{2^n}$-points on $\tilde{E}$. The degrees $n = 107$ and $n = 181$ of the extension fields turn out to be favourable in view of the desired criteria. The prime factorization of the corresponding orders N_n and $\tilde{N}_n$ are given as follows.

$$N_{107} = 2 \cdot 81129638414606692182851032212511$$
$$\tilde{N}_{107} = 4 \cdot 40564819207303335604363489037809$$

$$N_{181} = 2 \cdot 122719 \cdot 23531 \cdot 53069748316846439673094088911559937083526694 3$$
$$\tilde{N}_{181} = 4 \cdot 1087 \cdot 12671 \cdot 115117 \cdot 307339 \cdot 157243119770415559863682662828955381 3$$

The first example contains prime numbers with 32 decimal digits. This example is already mentioned in [3]. The second example contains prime numbers with 45 and 37 decimal digits, respectively.

References

[1] E. Brickell, D.M. Gordon, K.S. McCurley, D. Wilson, *Fast Exponentiation with Precomputation*, Eurocrypt'92, to appear.

[2] B.S. Kaliski, Jr., *One-way Permutations on Elliptic Curves*, Journal of Cryptology, Vol.3, No. 3, pp.187–199, 1991.

[3] N. Koblitz, *CM-Curves with Good Cryptographic Properties*, Advances in Cryptology—Crypto'91, Proceedings, pp. 279–287, Springer-Verlag, 1992.

[4] N. Koblitz, *Elliptic Curve Crypto Systems*, Math. of Computation, Vol. 48, pp. 203–209, 1987.

[5] N. Koblitz, *Hyperelliptic Cryptosystems*, Journal of Cryptology, Vol. 1, No. 3, pp. 139–150, 1989.

[6] A. Menezes, T. Okamoto, S.A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, Proceedings of the 23rd ACM Symp. Theory of Computing, 1991.

[7] V. Miller, *Use of Elliptic Curves in Cryptography*, Advances in Cryptology—Crypto'85, Proceedings, pp. 417–426, Springer-Verlag, 1986.

[8] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer-Verlag, 1986.