A note on twists for pairing friendly curves

Michael Scott

School of Computing
Dublin City University
Ballymun, Dublin 9, Ireland.
mike@computing.dcu.ie

1 Twists for pairings

As is well known a non-supersingular pairing-friendly elliptic curve is defined by p, t, r and k, where p is the prime field, t is the trace of the Frobenius and r is the pairing-friendly group size, where $r|p+1-t$, and $r|p^k-1$ for the smallest positive integer k, the embedding degree. For certain families of pairing-friendly curves, the parameters p, r and t can be represented as polynomials $p(x), r(x)$ and $t(x)$.

When implementing pairings on pairing friendly non-supersingular curves, one of the parameters is placed on the curve defined over the base field $\mathbb{F}_p$, and the other is typically placed on a 'twisted' curve, where there exists a group of points of order r which are isomorphic to a group of points on the curve defined over the full k-th extension of the base field. For example if the pairing is the ate pairing, or one of its variants, the pairing is $e(Q,P)$, where $Q \in E'(\mathbb{F}_{p^{k/d}})$, where k is the embedding degree and d is the degree of the twist. Points on the twisted curve are defined over a smaller field, and are thus obviously much faster to manipulate. However when required in the pairing calculation (for example for evaluation of the line function) they can be quickly mapped to a point on $E(\mathbb{F}_{p^k})$.

If the embedding degree k is even then the quadratic twist ($d=2$) can be used. If the pairing-friendly curve has a CM discriminant of $D=1$, and $4|k$, then we can use a quartic twist associated with $d=4$. Similarly if the curve has $D=3$, and $6|k$, then a sextic twist can be used $d=6$.

2 Using quadratic twists for pairings

Consider first the case of the quadratic twist with the elliptic curve in its standard Weierstrass representation.

$$y^2 = x^3 + Ax + B$$

In pairing-based cryptography $A, B \in \mathbb{F}_p$, although it is only when considered over $\mathbb{F}_{p^k}$ that the curve supports a bilinear pairing.

The twisted curve over the field of definition $\mathbb{F}_{p^{k/d}}$ will be (following Hess, Smart and Vercauteren [3])

$$y^2 = x^3 + Ax/i^2 + B/i^3$$

where i is any quadratic non-residue in the field of definition. Since the chosen QNR i appears here as a divisor, we call this a type D twist. To map from the twisted curve to the original curve

$$E' \to E : (x, y) \to (ix, i^{3/2}y)$$

This can be checked by simple substitution into the equation above. Often this type of mapping can be realised by a simple placement of x and y from the twisted curve into the structure representing the point on the original curve over $\mathbb{F}_{p^k}$, assuming that $x^k - i$ is also our choice for the irreducible polynomial used to represent the full extension field. This "untwisting" mapping is required for the line function evaluation in the calculation of the pairing, when we map a point from the twisted curve $E'(\mathbb{F}_{p^{k/d}})$ to the original curve $E(\mathbb{F}_{p^k})$. See below for a fully worked example.

For example if the embedding degree $k = 2$, the field of definition of the quadratic twist is $\mathbb{F}_p$, and $p = 3 \bmod 4$, then $i = -1$ is a good choice, and the twisted curve is simply

$$y^2 = x^3 + Ax - B$$

Alternatively if $p = 5 \bmod 8$, then $i = -2$ is a good choice, and the twisted curve is

$$y^2 = x^3 + (A/4)x - B/8$$

In either case $x^2 + 1$ or $x^2 + 2$ respectively makes a good choice for the irreducible binomial to represent $\mathbb{F}_{p^2}$.

If the embedding degree $k = 4$, the field of definition of the quadratic twist is the quadratic extension field $\mathbb{F}_{p^2}$, and if $p = 3 \bmod 8$, one can use $x^2 - (1+\sqrt{-1})$ as an irreducible polynomial for the towered representation of $\mathbb{F}_{p^4}$ [2], which immediately suggests $i = (1 + \sqrt{-1})$ as the quadratic non-residue to use in this case. If $p = 5 \bmod 8$, then $i = \sqrt{-2}$ is suitable.

Note that there is only one quadratic twist (different choices for i just result in isomorphic curves). Note also that from an implementation point of view it is important that the irreducible binomial be as simple as possible (as it will be used for extensive extension field arithmetic in the pairing calculation). It is less important that the equation of the curve be simple, as it is used primarily to place points on the curve. However it may impact in a small way on the complexity of the point addition/doubling formulae.

For example in the standard projective Jacobian coordinates, point doubling can exploit the case $A = -3$ to save a field multiplication. The numerator of the slope of the line in this case is calculated as $3X^2 + AZ^4$, which in the case $A = -3$ can be written as $3(X - Z^2)(X + Z^2)$. It might be feared that this nice property would be lost on the twist. However on the quadratic twist $A = -3/i^2$, and so the numerator of the slope can be calculated as $3(X - Z^2/i)(X + Z^2/i)$. Although

we don't like divisions, even by small constants, we can quite easily replace the division by a multiplications, by multiplying the numerator and denominator of the slope "above and below" by i^2

An alternative and perhaps simpler way to address this issue is to represent the twisted curve by the isomorphic curve

$$y^2 = x^3 + i^2Ax + i^3B$$

We call this a type M twist. To effect the mapping in this case

$$E' \rightarrow E : (x, y) \rightarrow (x/i, i^{1/2}y/i^2)$$

This results in a slightly more complex line function evaluation in the Miller loop, but for point doubling we are now using $A = -3i^2$, which avoids the division in a simpler way. Fortunately in the line function evaluation divisions can always be replaced by multiplications, as it is always possible to "clear denominators" by exploiting the denominator elimination optimization.

In this situation, for a given pairing friendly curve, either approach can be taken, the choice depends only on efficiency of implementation, and there seems little difference between the two.

3 Using sextic twists for pairings

In the case of sextic twists, following [3], there are actually two sextic twists, one with $q + 1 - (-3f + t)/2$ points on it, the other with $q + 1 - (3f + t)/2$, where $f = \sqrt{(4q - t^2)/3}$. One of these will be the "right" twist, whose order will be divisible by r, the predetermined size of the pairing-friendly group. The other is the "wrong" twist.

The equation for the type D sextic twist associated with our choice of i (from [3]) is

$$y^2 = x^3 + B/i$$

where i is a cubic and quadratic non-residue in the field of definition of the twist and $x^6 - i$ is irreducible. This may generate the curve with the right twist, but if it does not the other possibility (see [1]) is

$$y^2 = x^3 + B/i^5$$

which we can write as

$$y^2 = x^3 + i.B/i^6$$

But an isomorphic curve is the M-type twist

$$y^2 = x^3 + i.B$$

(recall we can use any suitable non-residue).

One of these twists will have the correct number of points on it, the other will not. We emphasise that this is not a choice – only one of them will work for a given choice of i and for a given pairing-friendly curve. We continue with the one that works. The set of all pairing friendly curves generated from a family of such curves will be divided (not necessarily evenly) between these two camps, so we might selectively choose one type over the other if there are advantages in doing so.

So in this case (unlike for the quadratic twist) we do not have a choice of which representation to use; the pairing friendly curve for the optimal choice of i falls into either the M-type or D-type category.

For the D-type twist we can move from the twisted curve back to the original curve using

$$E' \to E : (x, y) \to (i^{1/3}x, i^{1/2}y)$$

For the M-type twist the mapping is slightly more complicated

$$E' \to E : (x, y) \to (i^{2/3}x/i, i^{1/2}y/i)$$

Which twist is better for an implementation? Note that the point doubling formula is not affected at all in this case as $A = 0$ for these curves. However the line function evaluations will be impacted. The D-type twist is probably to be preferred, as the "untwisting" is simpler in that case.

4 Using quartic twists for pairings

In the case of quartic twists, there are two possibilities for the quartic twist, one with $q + 1 - f$ points on it, the other with $q + 1 + f$, where $f = \sqrt{(4q - t^2)/3}$. Only one will be pairing friendly and divisible by r. The equation for the D-type quartic twist (from [3]) is

$$y^2 = x^3 + Ax/i$$

where i is a quadratic non-residue in the field (and so $x^4 - i$ is irreducible. Again we choose i to be as simple as possible). This may be the twist with the embedded pairing-friendly group, but if it is not the other possibility is

$$y^2 = x^3 + Ax/i^3$$

which can be written as

$$y^2 = x^3 + i.Ax/i^4$$

But an isomorphic curve is the M-type twist

$$y^2 = x^3 + i.Ax$$

Either the D- or M-type twist will have the correct number of points on it, the other will not. We continue with the one that works. For the D-type twist we can move from the twisted curve back to the original curve using

$$E' \to E : (x, y) \to (i^{1/2}x, i^{3/4}y)$$

For the M-type twist the mapping is

$$E' \to E : (x, y) \to (i^{1/2}x/i, i^{1/4}y/i)$$

Which twist is better for implementation? The point doubling and line function calculations will be impacted. But the difference is negligible.

5 The Line Function

The twisting method has implications for the calculation of the line function, as required for the overall pairing calculation. Let us consider a specific example, the calculation of an ate pairing (or some variant of the ate pairing), using affine coordinates on a D-type twisted pairing friendly curve, embedding degree 18, with the extension field $\mathbb{F}_{p^{18}}$ represented using the irreducible polynomial $z^{18} + 2$. Such curves can easily be found using the construction given by [4]. We will represent the full extension field as recommended in [2] as a 1-3-6-18 tower.

Elements in $\mathbb{F}_{p^{18}}$ can then be represented as a triple of elements in $\mathbb{F}_{p^6}$

$$(a_0 + a_1 z^3) + (b_0 + b_1 z^3)z + (c_0 + c_1 z^3)z^2$$

where $a_0, a_1, b_0, b_1, c_0, c_1 \in \mathbb{F}_{p^3}$, and $z = (-2)^{1/18}$. We will write such an element as $\{a_0, a_1, b_0, b_1, c_0, c_1\}$.

Now for the ate pairing and its variants, the first parameter of the pairing lies on the twisted curve. Therefore the line is calculated on $E'(\mathbb{F}_{p^3})$. Assuming that it passes through the point (x, y) then this must be "untwisted" via the above mapping to the point (z^2x, z^3y) (with coordinates in $\mathbb{F}_{p^{18}}$) in order to calculate the line function. So $x \to \{0, 0, 0, 0, x, 0\}$, $y \to \{0, y, 0, 0, 0, 0\}$. The line slope $\lambda \in \mathbb{F}_{p^3}$ from the point addition or doubling on $E'(\mathbb{F}_{p^3})$, arising as it does from a quotient of y and x, also needs to be untwisted to $z\lambda$, and hence becomes $\lambda \to \{0, 0, \lambda, 0, 0, 0\}$.

The second parameter of the pairing is a fixed point on the base field (x_p, y_p), where $x_p, y_p \in \mathbb{F}_p$. Finally the line function is calculated as

$$(y - y_p) - \lambda(x - x_p)$$

which evaluates as $\{-y_p, y - x\lambda, x_p\lambda, 0, 0, 0\}$. Observe that this requires only a very small amount of $\mathbb{F}_{p^3}$ arithmetic (primarily a single multiplication) followed by a placement into the $\mathbb{F}_{p^{18}}$ structure.

6 How to proceed?

We suggest the following to ensure an efficient implementation.

First choose an optimal representation for the irreducible binomial $x^k - i$, that is i with the simplest form. The bulk of pairing arithmetic will be with respect to this binomial, and so reduction should be as simple as possible.

Having chosen i, next find a suitable pairing-friendly curve. For the quartic and sextic twist cases, one might either decide to stick with one form of the twist or the other – simply rejecting curves which require the "wrong" twist for our preferred choice of i. Alternatively one might might decide to support both forms, as there may be other criteria that are more important – like finding the Miller control variable with minimum Hamming weight. However the point doubling and line function evaluations in both cases may be slightly different (as the twisting and untwisting mappings will be different), and so the implementation must change to support one form or the other.

Note that this is at variance with the advice given in [1], where the authors suggest choosing the curve first and then finding the correct twist, and finally letting these choices dictate the choice of irreducible polynomial.

References

1. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC'2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer-Verlag, 2006.
2. N. Benger and M. Scott. Constructing tower extensions for the implementation of pairing-based cryptography. In *WAIFI 2010*, volume 6087 of *Lecture Notes in Computer Science*, pages 180–195. Springer-Verlag, 2010.
3. F. Hess, N. Smart, and F. Vercauteren. The eta pairing revisted. *IEEE Trans. Information Theory*, 52:4595–4602, 2006.
4. E. Kachisa, E. Schaefer, and M. Scott. Constructing brezing-weng pairing friendly elliptic curves using elements in the cyclotomic field. In *Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer-Verlag, 2008.