Twisting Edwards curves with isogenies

Mike Hamburg[*]

Abstract

Edwards' elliptic curve form is popular in modern cryptographic implementations thanks to their fast, strongly unified addition formulas. Twisted Edwards curves with $a = -1$ are slightly faster, but their addition formulas are not complete over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$. In this short note, we propose that designers specify Edwards curves, but implement scalar multiplications and the like using an isogenous twisted Edwards curve.

1 Edwards curves

Edwards and Twisted Edwards elliptic curves [4, 3, 6] have the form

$$\mathcal{E}_{d,a}: \quad y^2 + a \cdot x^2 = 1 + d \cdot x^2 \cdot y^2$$

over some field $\mathbb{F}$, with $d, a \neq 0$. Their identity is $(0, 1)$, and they have a point of order 2 at $(0, -1)$. For speed and simplicity, most authors choose $a \in \{\pm 1\}$, so we will consider only those values of a. In this paper, we will call the curve "twisted" when $a = -1$ and "untwisted" when $a = 1$.

When d is square in $\mathbb{F}$, the curve $\mathcal{E}_{d,a}$ has a point of order 4 with $y = \infty$. Likewise, when d/a is square in $\mathbb{F}$, it has a point of order 2 with $x = \infty$. When a is square in $\mathbb{F}$, it has points of order 4 with $y = 0$, such as $(\pm 1, 0)$ when $a = 1$.

The addition formula on $\mathcal{E}_{d,a}$ is

$$(x_1, y_1) + (x_2, y_2) \quad = \quad \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \;\; \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

This formula is correct when neither the inputs nor outputs include points at infinity [6]. For $a = 1$, it may be computed with 9 full field multiplications, plus 1 multiplication by d (which might be small for efficiency) and 7 additions. When $a = -1$, it may be computed with 8

[*] Cryptography Research, a division of Rambus.

full field multiplications, 1 multiplication by d and 8 additions [6]. Thus, twisted Edwards curves are generally faster than untwisted ones. As a special case, the doubling formulas are

$$2 \cdot (x, y) \quad = \quad \left(\frac{2xy}{1 + dx^2y^2}, \ \frac{y^2 - ax^2}{1 - dx^2y^2} \right) \quad = \quad \left(\frac{2xy}{y^2 + ax^2}, \ \frac{y^2 - ax^2}{2 - y^2 - ax^2} \right)$$

For a field $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$, the addition formulas above are not complete for twisted Edwards curves, because either d or $d/a = -d$ is square in $\mathbb{F}$. This pitfall can be avoided by choosing a curve $\mathcal{E}$ of order $4 \cdot q$ with q prime, and working only in the q-torsion subgroup [5, 6]. This is often done anyway; for example, the system Curve25519 [2] begins with 3 doublings in order to clear its cofactor of 8. Still, it may not always be practical to work in the q-torsion subgroup. Or even if it is practical, designers may wish to specify curves with as few pitfalls as possible.

2 An isogeny

Fortunately, there is a simple way to obtain the speed of a twisted Edwards curve with the simplicity of an untwisted one. This is because the map $\phi_a : \mathcal{E}_{d,a} \to \mathcal{E}_{d-a,-a}$ specified by

$$(x, y) \to \left(\frac{2xy}{y^2 - ax^2}, \frac{y^2 + ax^2}{2 - y^2 - ax^2} \right)$$

is a 4-isogeny between the two curves, with dual isogeny ϕ_{-a}. We derived this isogeny from those found in [1]. If we choose an untwisted curve $\mathcal{E}_{d,1}$ of order $4 \cdot q$ with q prime (and thus, d nonsquare in $\mathbb{F}$), then we see that all the 4-torsion points of $\mathcal{E}_{d,1}$ are all in the kernel of the isogeny. Therefore, its image is the q-torsion group of the twisted Edwards curve $\mathcal{E}_{d-1,-1}$. Afterward, the faster twisted Edwards curve formulas can be used without the possibility of exceptions.

Computing ϕ_1 or its dual ϕ_{-1} takes about the same amount of time as a doubling on either curve. In other words, if a designer plans to clear the 4-torsion on $\mathcal{E}_{d,1}$ with two doublings, then applying the isogeny and its dual is just as effective and costs the same.

3 A strategy

We suggest, therefore, that when $p \equiv 3 \pmod 4$, Edwards systems should specified on an untwisted Edwards curve $\mathcal{E}_{d,1}$ with order $4 \cdot q$, where q is prime. This implies that d is not square over $\mathbb{F}$. (There will of course be other security requirements and desiderata.) Short-running operations on this curve can then take advantage of the complete untwisted Edwards formulas, and straightforward implementations will not encounter the pitfalls present on twisted curves.

For longer-running operations, such as a scalar multiplication $P \to s \cdot P$, implementers then have the option of using the isogenous twisted curve. For example, they might compute

$$s \cdot P = (s \bmod 4) \cdot P + \phi_{-1}\left(\left\lfloor \frac{s}{4} \right\rfloor \cdot \phi_1(P)\right)$$

Commonly, s is known ahead of time to be a multiple of 4, in which case this simplifies to

$$s \cdot P = \phi_{-1}\left((s/4) \cdot \phi_1(P)\right)$$

Alternatively, if P is known ahead of time to be a q-torsion point, the formula

$$s \cdot P = \phi_{-1}\left((s \cdot 4^{-1} \bmod q) \cdot \phi_1(P)\right)$$

can be used. The same techniques can be used for a linear combination $s \cdot P + t \cdot Q$, and for a fixed-based scalar multiply. These formulas add either nothing or only a small amount to the cost of the operation on $\mathcal{E}_{d-1,-1}$.

4 Impact

The twisted Edwards addition formulas take 8 multiplications instead of 9, making them about 10% faster depending on the field implementation. The total speedup in a larger computation will depend on the fraction of time taken to perform additions, rather than doublings, inversions, etc.

Since variable-base scalar multiplies are dominated by repeated doubling, our strategy only reduces the time taken by about 3% in total. The savings rise to about 5% for double-base combinations, and 8% for fixed-base scalar multiplies.

5 Future work

We are curious whether ϕ_1 and ϕ_{-1} can profitably be combined with point decompression and compression formulas, respectively.

References

[1] Omran Ahmadi and Robert Granger. On isogeny classes of edwards curves over finite fields. Cryptology ePrint Archive, Report 2011/135, 2011. http://eprint.iacr.org/2011/135.

[2] D. Bernstein. Curve25519: new Diffie-Hellman speed records. *Public Key Cryptography-PKC 2006*, pages 207–228, 2006.

[3] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted edwards curves. *Progress in Cryptology–AFRICACRYPT 2008*, pages 389–405, 2008.

[4] H.M. Edwards. A normal form for elliptic curves. *Bulletin-American Mathematical Society*, 44(3):393, 2007.

[5] Mike Hamburg. Fast and compact elliptic-curve cryptography. Cryptology ePrint Archive, Report 2012/309, 2012. http://eprint.iacr.org/2012/309.

[6] H. Hışıl, K. Wong, G. Carter, and E. Dawson. Twisted edwards curves revisited. *Advances in Cryptology–ASIACRYPT 2008*, pages 326–343, 2008.