Twisted Edwards Curves

Daniel J. Bernstein[1], Peter Birkner[2], Tanja Lange[2], and Christiane Peters[2]

[1] Department of Mathematics, Statistics, and Computer Science (M/C 249)
University of Illinois at Chicago, Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
p.birkner@tue.nl, tanja@hyperelliptic.org, c.p.peters@tue.nl

Abstract. This paper introduces "twisted Edwards curves," a generalization of the recently introduced Edwards curves; shows that twisted Edwards curves include more curves over finite fields, and in particular every elliptic curve in Montgomery form; presents fast explicit formulas for twisted Edwards curves in projective and inverted coordinates; and shows that twisted Edwards curves save time for many curves that were already expressible as Edwards curves.

Keywords: Elliptic curves, Edwards curves, twisted Edwards curves, Montgomery curves

1 Introduction

Edwards in [7], generalizing an example from Euler and Gauss, introduced an addition law for the curves $x^2 + y^2 = c^2(1 + x^2y^2)$ over a non-binary field k. Edwards showed that every elliptic curve over k can be expressed in the form $x^2 + y^2 = c^2(1 + x^2y^2)$ if k is algebraically closed. However, over a finite field, only a small fraction of elliptic curves can be expressed in this form.

Bernstein and Lange in [4] presented fast explicit formulas for addition and doubling in coordinates $(X : Y : Z)$ representing $(x, y) = (X/Z, Y/Z)$ on an Edwards curve, and showed that these explicit formulas save time in elliptic-curve cryptography. Bernstein and Lange also generalized the addition law to the curves $x^2 + y^2 = c^2(1 + dx^2y^2)$. This shape covers considerably more elliptic curves over a finite field than $x^2+y^2 = c^2(1+x^2y^2)$. All curves in the generalized form are isomorphic to curves $x^2 + y^2 = 1 + dx^2y^2$.

In this paper, we further generalize the Edwards addition law to cover all curves $ax^2+y^2 = 1+dx^2y^2$. Our fast explicit formulas for addition and doubling are almost as fast in the general case as they are for the special case $a = 1$. We

* Permanent ID of this document: c798703ae3ecfdc375112f19dd0787e4. Date of this document: 2008.01.08. This work has been supported in part by the European Commission through the IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498. This work was carried out while the authors were visiting INRIA Lorraine (LORIA).

show that our generalization brings the speed of the Edwards addition law to every Montgomery curve; we also show that, over prime fields $\mathbf{F}_p$ where $p \equiv 1 \pmod 4$, many Montgomery curves are not covered by the special case $a = 1$. Our generalization is also of interest for many curves that were already expressible in Edwards form; we explain how the twisting can save time in arithmetic. In [2] we successfully applied twisted Edwards curves to the elliptic-curve method of factorization.

Section 2 reviews Edwards curves, introduces twisted Edwards curves, and shows that each twisted Edwards curve is (as the name would suggest) a twist of an Edwards curve. Section 3 shows that every Montgomery curve can be expressed as a twisted Edwards curve, and vice versa. Section 4 reports the percentages of elliptic curves (over various prime fields) that can be expressed as Edwards curves, twisted Edwards curves, "4 times odd" twisted Edwards curves, etc. Section 5 generalizes the Edwards addition law, the explicit formulas from [4], and the "inverted" formulas from [5] to handle twisted Edwards curves. Section 6 analyzes the benefits of the generalization for cryptographic applications.

2 Edwards curves and twisted Edwards curves

In this section we briefly review Edwards curves and the Edwards addition law at the level of generality of [4]. We then introduce twisted Edwards curves and discuss their relationship to Edwards curves.

2.1. Review of Edwards curves. Throughout the paper we consider elliptic curves over a non-binary field k, i.e., a field k in which $2 \neq 0$, i.e., a field k whose characteristic $\operatorname{char}(k)$ is not 2.

An Edwards curve over k is a curve $E : x^2 + y^2 = 1 + dx^2y^2$ where $d \in k - \{0, 1\}$. The sum of two points (x_1, y_1), (x_2, y_2) on this Edwards curve E is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

This addition law is strongly unified: i.e., it can also be used to double a point. If d is a nonsquare in k then, as proven in [4, Theorem 3.3], this addition law is complete: it works for all pairs of inputs. The point $(0, 1)$ is the neutral element of the addition law. The point $(0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4. The inverse of a point (x_1, y_1) on E is $(-x_1, y_1)$.

2.2. Twisted Edwards curves. The existence of points of order 4 restricts the number of elliptic curves in Edwards form over k. We embed the set of Edwards curves in a larger set of elliptic curves of a similar shape by introducing twisted Edwards curves.

Definition 2.3 (twisted Edwards curve). *Fix a field k with* $\operatorname{char}(k) \neq 2$. *Fix distinct nonzero elements $a, d \in k$. The* twisted Edwards curve with coefficients a and d *is the curve*

$$\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

An Edwards curve *is a twisted Edwards curve with* $a = 1$.

In Section 3 we will show that every twisted Edwards curve is birationally equivalent to an elliptic curve in Montgomery form, and vice versa.

2.4. Twisted Edwards curves as twists of Edwards curves. The twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is a quadratic twist of the Edwards curve $\mathrm{E}_{\mathrm{E},1,d/a} : \bar{x}^2 + \bar{y}^2 = 1 + (d/a)\bar{x}^2\bar{y}^2$. The map $(\bar{x}, \bar{y}) \mapsto (x, y) = (\bar{x}/\sqrt{a}, \bar{y})$ is an isomorphism from $\mathrm{E}_{\mathrm{E},1,d/a}$ to $\mathrm{E}_{\mathrm{E},a,d}$ over $k(\sqrt{a})$. If a is a square in k then $\mathrm{E}_{\mathrm{E},a,d}$ is isomorphic to $\mathrm{E}_{\mathrm{E},1,d/a}$ over k.

More generally, $\mathrm{E}_{\mathrm{E},a,d}$ is a quadratic twist of $\mathrm{E}_{\mathrm{E},\bar{a},\bar{d}}$ for any $\bar{a}, \bar{d}$ satisfying $\bar{d}/\bar{a} = d/a$. Conversely, every quadratic twist of a twisted Edwards curve is isomorphic to a twisted Edwards curve; i.e., the set of twisted Edwards curves is invariant under quadratic twists.

Furthermore, the twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is a quadratic twist of the twisted Edwards curve $\mathrm{E}_{\mathrm{E},d,a} : d\bar{x}^2 + \bar{y}^2 = 1 + a\bar{x}^2\bar{y}^2$. The map $(\bar{x}, \bar{y}) \mapsto (x, y) = (\bar{x}, 1/\bar{y})$ is a birational equivalence from $\mathrm{E}_{\mathrm{E},d,a}$ to $\mathrm{E}_{\mathrm{E},a,d}$. More generally, $\mathrm{E}_{\mathrm{E},a,d}$ is a quadratic twist of $\mathrm{E}_{\mathrm{E},\bar{a},\bar{d}}$ for any $\bar{a}, \bar{d}$ satisfying $\bar{d}/\bar{a} = a/d$. This generalizes the known fact, used in [4, proof of Theorem 2.1], that $\mathrm{E}_{\mathrm{E},1,d}$ is a quadratic twist of $\mathrm{E}_{\mathrm{E},1,1/d}$.

3 Montgomery curves and twisted Edwards curves

Let k be a field with $\mathrm{char}(k) \neq 2$. In this section we show that the set of Montgomery curves over k is equivalent to the set of twisted Edwards curves over k. We also analyze the extent to which this is true without twists.

Definition 3.1 (Montgomery curve). *Fix a field* k *with* $\mathrm{char}(k) \neq 2$. *Fix* $A \in k - \{-2, 2\}$ *and* $B \in k - \{0\}$. *The* Montgomery curve with coefficients A and B *is the curve*

$$\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3 + Au^2 + u.$$

Theorem 3.2. *Fix a field* k *with* $\mathrm{char}(k) \neq 2$.

(i) Every twisted Edwards curve over k *is birationally equivalent over* k *to a Montgomery curve.*

Specifically, fix distinct nonzero elements $a, d \in k$. *The twisted Edwards curve* $\mathrm{E}_{\mathrm{E},a,d}$ *is birationally equivalent to the Montgomery curve* $\mathrm{E}_{\mathrm{M},A,B}$, *where* $A = 2(a + d)/(a - d)$ *and* $B = 4/(a - d)$. *The map* $(x, y) \mapsto (u, v) = ((1 + y)/(1 - y), (1 + y)/(1 - y)x)$ *is a birational equivalence from* $\mathrm{E}_{\mathrm{E},a,d}$ *to* $\mathrm{E}_{\mathrm{M},A,B}$, *with inverse* $(u, v) \mapsto (x, y) = (u/v, (u - 1)/(u + 1))$.

(ii) Conversely, every Montgomery curve over k *is birationally equivalent over* k *to a twisted Edwards curve.*

Specifically, fix $A \in k - \{-2, 2\}$ *and* $B \in k - \{0\}$. *The Montgomery curve* $\mathrm{E}_{\mathrm{M},A,B}$ *is birationally equivalent to the twisted Edwards curve* $\mathrm{E}_{\mathrm{E},a,d}$, *where* $a = (A + 2)/B$ *and* $d = (A - 2)/B$.

Proof. (i) Note that A and B are defined, since $a \neq d$. Note further that $A \in k-\{-2,2\}$ and $B \in k-\{0\}$: if $A = 2$ then $a+d = a-d$ so $d = 0$, contradiction; if $A = -2$ then $a+d = d-a$ so $a = 0$, contradiction. Thus $\mathrm{E}_{\mathrm{M},A,B}$ is a Montgomery curve.

The following script for the SAGE computer-algebra system checks, in the function field of the curve $\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$, that the quantities $u = (1+y)/(1-y)$ and $v = (1+y)/(1-y)x$ satisfy $Bv^2 = u^3 + Au^2 + u$:

```
R.<a,d,x,y>=QQ[]
A=2*(a+d)/(a-d)
B=4/(a-d)
S=R.quotient(a*x^2+y^2-(1+d*x^2*y^2))
u=(1+y)/(1-y)
v=(1+y)/((1-y)*x)
0==S((B*v^2-u^3-A*u^2-u).numerator())
```

The exceptional cases $y = 1$ and $x = 0$ occur for only finitely many points (x, y) on $\mathrm{E}_{\mathrm{E},a,d}$. Conversely, $x = u/v$ and $y = (u-1)/(u+1)$; the exceptional cases $v = 0$ and $u = -1$ occur for only finitely many points (u, v) on $\mathrm{E}_{\mathrm{M},A,B}$.

(ii) Note that a and d are defined, since $B \neq 0$. Note further that $a \neq 0$ since $A \neq -2$; $d \neq 0$ since $A \neq 2$; and $a \neq d$. Thus $\mathrm{E}_{\mathrm{E},a,d}$ is a twisted Edwards curve. Furthermore

$$2\frac{a+d}{a-d} = 2\frac{\frac{A+2}{B} + \frac{A-2}{B}}{\frac{A+2}{B} - \frac{A-2}{B}} = A \quad \text{and} \quad \frac{4}{(a-d)} = \frac{4}{\frac{A+2}{B} - \frac{A-2}{B}} = B.$$

Hence $\mathrm{E}_{\mathrm{E},a,d}$ is birationally equivalent to $\mathrm{E}_{\mathrm{M},A,B}$ by (i). □

3.3. Exceptional points for the birational equivalence. The map $(u, v) \mapsto (u/v, (u-1)/(u+1))$ from $\mathrm{E}_{\mathrm{M},A,B}$ to $\mathrm{E}_{\mathrm{E},a,d}$ in Theorem 3.2 is undefined at the points of $\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3 + Au^2 + u$ with $v = 0$ or $u + 1 = 0$. We investigate these points in more detail:

- The point $(0, 0)$ on $\mathrm{E}_{\mathrm{M},A,B}$ corresponds to the affine point of order 2 on $\mathrm{E}_{\mathrm{E},a,d}$, namely $(0, -1)$. This point and $(0, 1)$ are the only exceptional points of the inverse map $(x, y) \mapsto ((1+y)/(1-y), (1+y)/(1-y)x)$, where $(0, 1)$ is mapped to the point at infinity.
- If $(A+2)(A-2)$ is a square (i.e., if ad is a square) then there are two more points with $v = 0$, namely $((-A \pm \sqrt{(A+2)(A-2)})/2, 0)$. These points have order 2. These points correspond to two points of order 2 at infinity on the desingularization of $\mathrm{E}_{\mathrm{E},a,d}$.
- If $(A-2)/B$ is a square (i.e., if d is a square) then there are two points with $u = -1$, namely $(-1, \pm\sqrt{(A-2)/B})$. These points have order 4. These points correspond to two points of order 4 at infinity on the desingularization of $\mathrm{E}_{\mathrm{E},a,d}$.

3.4. Eliminating the twists. Every Montgomery curve $\mathrm{E}_{\mathrm{M},A,B}$ is birationally equivalent to a twisted Edwards curve by Theorem 3.2, and therefore to a

quadratic twist of an Edwards curve. In other words, there is a quadratic twist of $\mathrm{E}_{\mathrm{M},A,B}$ that is birationally equivalent to an Edwards curve.

We now state two situations in which twisting is not necessary. Theorem 3.5 states that every elliptic curve having a point of order 4 is birationally equivalent to an Edwards curve. Theorem 3.6 states that, over a finite field k with $\#k \equiv 3 \pmod 4$, every Montgomery curve is birationally equivalent to an Edwards curve.

Some special cases of these results were already known. Bernstein and Lange proved in [4, Theorem 2.1(1)] that every elliptic curve having a point of order 4 is birationally equivalent to a twist of an Edwards curve, and in [4, Theorem 2.1(3)] that, over a finite field, every elliptic curve having a point of order 4 and a unique point of order 2 is birationally equivalent to an Edwards curve. We prove that the twist in [4, Theorem 2.1(1)] is unnecessary, and that the unique point of order 2 in [4, Theorem 2.1(3)] is unnecessary.

Theorem 3.5. *Fix a field k with $\mathrm{char}(k) \neq 2$. Let E be an elliptic curve over k. The group $E(k)$ has an element of order 4 if and only if E is birationally equivalent over k to an Edwards curve.*

Proof. Assume that E is birationally equivalent over k to an Edwards curve $\mathrm{E}_{\mathrm{E},1,d}$. The elliptic-curve addition law corresponds to the Edwards addition law; see [4, Theorem 3.2]. The point $(1, 0)$ on $\mathrm{E}_{\mathrm{E},1,d}$ has order 4, so E must have a point of order 4.

Conversely, assume that E has a point (u_4, v_4) of order 4. As in [4, Theorem 2.1, proof], assume without loss of generality that E has the form $v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u$; and define $d = 1 - 4u_4^3/v_4^2$.

The following script for the SAGE computer-algebra system checks, in the function field of E, that the quantities $x = v_4 u/u_4 v$ and $y = (u - u_4)/(u + u_4)$ satisfy $x^2 + y^2 = 1 + dx^2y^2$:

```
R.<u,v,u4,v4>=QQ[]
d=1-4*u4^3/v4^2
S=R.quotient((v^2-u^3-(v4^2/u4^2-2*u4)*u^2-u4^2*u).numerator())
x=v4*u/(u4*v)
y=(u-u4)/(u+u4)
0==S((x^2+y^2-1-d*x^2*y^2).numerator())
```

The exceptional cases $u_4 v = 0$ and $u = -u_4$ occur for only finitely many points (u, v) on E. Conversely, $u = u_4(1 + y)/(1 - y)$ and $v = v_4(1 + y)/(1 - y)x$; the exceptional cases $y = 1$ and $x = 0$ occur for only finitely many points (x, y) on $\mathrm{E}_{\mathrm{E},1,d}$.

Therefore the rational map $(u, v) \mapsto (x, y) = (v_4 u/u_4 v, (u - u_4)/(u + u_4))$, with inverse $(x, y) \mapsto (u, v) = (u_4(1+y)/(1-y), v_4(1+y)/(1-y)x)$, is a birational equivalence from E to the Edwards curve $\mathrm{E}_{\mathrm{E},1,d}$. □

Theorem 3.6. *If k is a finite field with $\#k \equiv 3 \pmod 4$ then every Montgomery curve over k is birationally equivalent over k to an Edwards curve.*

Proof. Fix $A \in k - \{-2, 2\}$ and $B \in k - \{0\}$. We will use an idea of Okeya, Kurumatani, and Sakurai [12], building upon the observations credited to Suyama in [11, page 262], to prove that the Montgomery curve $\mathrm{E}_{\mathrm{M},A,B}$ has a point of order 4. This fact can be extracted from [12, Theorem 1] when $\#k$ is prime, but to keep this paper self-contained we include a direct proof.

Case 1: $(A+2)/B$ is a square. Then (as in Section 3.3) $\mathrm{E}_{\mathrm{M},A,B}$ has a point $(1, \sqrt{(A+2)/B})$ of order 4.

Case 2: $(A+2)/B$ is a nonsquare but $(A-2)/B$ is a square. Then $\mathrm{E}_{\mathrm{M},A,B}$ has a point $(-1, \sqrt{(A-2)/B})$ of order 4.

Case 3: $(A+2)/B$ and $(A-2)/B$ are nonsquares. Then $(A+2)(A-2)$ must be square, since k is finite. The Montgomery curve $\mathrm{E}_{\mathrm{M},A,A+2}$ has three points $(0,0)$, $((-A \pm \sqrt{(A+2)(A-2)})/2, 0)$ of order 2, and a point $(1,1)$ of order 4, so $\#\mathrm{E}_{\mathrm{M},A,A+2}(k) \equiv 0 \pmod 8$. Furthermore, $\mathrm{E}_{\mathrm{M},A,B}$ is a nontrivial quadratic twist of $\mathrm{E}_{\mathrm{M},A,A+2}$, so $\#\mathrm{E}_{\mathrm{M},A,B}(k) + \#\mathrm{E}_{\mathrm{M},A,A+2}(k) = 2\#k + 2 \equiv 0 \pmod 8$. Therefore $\#\mathrm{E}_{\mathrm{M},A,B}(k) \equiv 0 \pmod 8$. The curve $\mathrm{E}_{\mathrm{M},A,B}$ cannot have more than three points of order 2, so it must have a point of order 4.

In every case $\mathrm{E}_{\mathrm{M},A,B}$ has a point of order 4. By Theorem 3.5, $\mathrm{E}_{\mathrm{M},A,B}$ is birationally equivalent to an Edwards curve. □

This theorem does not generalize to $\#k \equiv 1 \pmod 4$. For example, the Montgomery curve $\mathrm{E}_{\mathrm{M},9,1}$ over $\mathbf{F}_{17}$ has order 20 and group structure isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/10$. This curve is birationally equivalent to the twisted Edwards curve $\mathrm{E}_{\mathrm{E},11,7}$, but it does not have a point of order 4, so it is not birationally equivalent to an Edwards curve.

Theorem 3.7. *Let k be a finite field with $\#k \equiv 1 \pmod 4$. Let $\mathrm{E}_{\mathrm{M},A,B}$ be a Montgomery curve so that $(A+2)(A-2)$ is a square and let δ be a nonsquare.*

Exactly one of $\mathrm{E}_{\mathrm{M},A,B}$ and its nontrivial quadratic twist $\mathrm{E}_{\mathrm{M},A,\delta B}$ is birationally equivalent to an Edwards curve.

In particular, $\mathrm{E}_{\mathrm{M},A,A+2}$ is birationally equivalent to an Edwards curve.

Proof. Since $(A+2)(A-2)$ is a square both $\mathrm{E}_{\mathrm{M},A,B}$ and $\mathrm{E}_{\mathrm{M},A,\delta B}$ contain a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. This subgroup accounts for a factor of 4 in the group order. Since $\#\mathrm{E}_{\mathrm{M},A,B}(k) + \#\mathrm{E}_{\mathrm{M},A,\delta B}(k) = 2\#k + 2 \equiv 4 \pmod 8$ exactly one of $\#\mathrm{E}_{\mathrm{M},A,B}(k)$ and $\#\mathrm{E}_{\mathrm{M},A,\delta B}(k)$ is divisible by 4 but not by 8. That curve cannot have a point of order 4 while the other one has a point of order 4. The first statement follows from Theorem 3.5.

The second statement also follows from Theorem 3.5, since the point $(1,1)$ on $\mathrm{E}_{\mathrm{M},A,A+2}$ has order 4. □

4 Statistics

It is well known that, when p is a large prime, there are approximately $2p$ isomorphism classes of elliptic curves over the finite field $\mathbf{F}_p$. How many of these elliptic curves are birationally equivalent to twisted Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$? How many are birationally equivalent to Edwards curves $x^2 + y^2 =$

$1 + dx^2y^2$? How many are birationally equivalent to complete Edwards curves, i.e., Edwards curves with nonsquare d? How do the statistics vary with the number of powers of 2 in the group order?

We computed the answers for various primes p by enumerating all complete Edwards curves, all Edwards curves, all twisted Edwards curves (with a limited set of a's covering all isomorphism classes), and all elliptic curves in Weierstrass form (with similar limitations). We transformed each curve to a birationally equivalent elliptic curve E and then computed $(\#E, j(E))$, where $\#E$ is the number of points on E and $j(E)$ is the j-invariant of E. Recall that $j(E) = j(E')$ if and only if E' is a twist of E, and that twists are distinguished by $\#E$ except for a few isomorphism classes.

Some parts of these experiments have been carried out before. See, e.g., [8]. However, the information in the literature is not sufficient for our comparison of Edwards curves (and complete Edwards curves) to twisted Edwards curves.

4.1. Answers for primes $p \equiv 1 \pmod 4$. For $p = 1009$ we found

- 504 different pairs $(\#E, j(E))$ for complete Edwards curves,
- 673 different pairs $(\#E, j(E))$ for Edwards curves,
- 842 different pairs $(\#E, j(E))$ for twisted Edwards curves, and
- 2014 different pairs $(\#E, j(E))$ for elliptic curves.

We looked more closely at the number of powers of 2 dividing $\#E$ and observed the following distribution:

Curves	Total	odd	$2 \cdot$ odd	$4 \cdot$ odd	$8 \cdot$ odd	$16 \cdot$ odd	$32 \cdot$ odd	$64 \cdot$ odd
complete Edwards	504	0	0	252	130	66	24	16
Edwards	673	0	0	252	195	122	42	30
twisted Edwards	842	0	0	421	195	122	42	30
all	2014	676	496	421	195	122	42	30

We observed similar patterns for more than 400 tested primes $p \equiv 1 \pmod 4$:

Curves	Total	odd	$2 \cdot$ odd	$4 \cdot$ odd	$8 \cdot$ odd
complete Edwards	$\approx (1/2)p$	0	0	$\approx (1/4)p$	$\approx (1/8)p$
Edwards	$\approx (2/3)p$	0	0	$\approx (1/4)p$	$\approx (3/16)p$
twisted Edwards	$\approx (5/6)p$	0	0	$\approx (5/12)p$	$\approx (3/16)p$
all	$\approx 2p$	$\approx (2/3)p$	$\approx (1/2)p$	$\approx (5/12)p$	$\approx (3/16)p$

We do not claim novelty for statistics regarding the set of Montgomery curves (in other words, the set of twisted Edwards curves) and the set of all elliptic curves; all of these statistics have been observed before, and some of them have been proven. See, e.g., [8]. Furthermore, the $(1/2)p$ for complete Edwards curves was pointed out in [4, Abstract]. However, the $(2/3)p$, $(1/4)p$, and $(3/16)p$ for Edwards curves appear to be new observations. We include the old statistics as a basis for comparison.

4.2. Answers for primes $p \equiv 3 \pmod 4$. For primes $p \equiv 3 \pmod 4$ the patterns are different, as one would expect from Theorems 3.6 and 3.7. For

example, here is the analogous table for $p = 1019$:

Curves	Total	odd	$2 \cdot$ odd	$4 \cdot$ odd	$8 \cdot$ odd	$16 \cdot$ odd	$32 \cdot$ odd	$64 \cdot$ odd
complete Edwards	490	0	0	236	127	68	33	10
Edwards	744	0	0	236	254	136	66	20
twisted Edwards	744	0	0	236	254	136	66	20
all	2012	680	510	314	254	136	66	20

We observed similar patterns for more than 400 tested primes $p \equiv 3 \pmod 4$:

Curves	Total	odd	$2 \cdot$ odd	$4 \cdot$ odd	$8 \cdot$ odd
complete Edwards	$\approx (1/2)p$	0	0	$\approx (1/4)p$	$\approx (1/8)p$
Edwards	$\approx (3/4)p$	0	0	$\approx (1/4)p$	$\approx (1/4)p$
twisted Edwards	$\approx (3/4)p$	0	0	$\approx (1/4)p$	$\approx (1/4)p$
all	$\approx 2p$	$\approx (2/3)p$	$\approx (1/2)p$	$\approx (1/3)p$	$\approx (1/4)p$

As above, we do not claim novelty for statistics regarding the set of Montgomery curves and the set of all elliptic curves; we include these statistics as a basis for comparison.

4.3. Near-prime group orders. We also looked at how often the odd part of $\#E$ was prime and observed the following distribution for $p = 1009$:

Curves	prime	$2 \cdot$ prime	$4 \cdot$ prime	$8 \cdot$ prime	$16 \cdot$ prime	$32 \cdot$ prime
complete Edwards	0	0	64	42	28	8
Edwards	0	0	64	63	50	14
twisted Edwards	0	0	102	63	50	14
all	189	98	102	63	50	14

Here is the analogous table for $p = 1019$:

Curves	prime	$2 \cdot$ prime	$4 \cdot$ prime	$8 \cdot$ prime	$16 \cdot$ prime	$32 \cdot$ prime
complete Edwards	0	0	48	25	22	9
Edwards	0	0	48	50	44	18
twisted Edwards	0	0	48	50	44	18
all	148	100	64	50	44	18

Of course, larger primes p have smaller chances of prime $\#E$, smaller chances of prime $\#E/2$, etc.

5 Arithmetic on twisted Edwards curves

In this section we present fast explicit formulas for addition and doubling on twisted Edwards curves.

5.1. The twisted Edwards addition law. Let $(x_1, y_1), (x_2, y_2)$ be points on the twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$. The sum of these points on $\mathrm{E}_{\mathrm{E},a,d}$ is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

The neutral element is $(0,1)$, and the negative of (x_1,y_1) is $(-x_1,y_1)$.

For the correctness of the addition law observe that it coincides with the Edwards addition law on $\bar{x}^2+y^2=1+(d/a)\bar{x}^2y^2$ with $\bar{x}=\sqrt{a}x$ which is proven correct in [4, Section 3].

These formulas also work for doubling. These formulas are complete (i.e., have no exceptional cases) if a is a square in k and d is a nonsquare in k. The latter follows from $\mathrm{E}_{\mathrm{E},a,d}$ being isomorphic to $\mathrm{E}_{\mathrm{E},1,d/a}$; d/a being a nonsquare in k and from [4, Theorem 3.1] which showed that the Edwards addition law is complete on $\mathrm{E}_{\mathrm{E},1,d'}$ if d' is a nonsquare.

5.2. Projective twisted Edwards coordinates. To avoid inversions we work on the projective twisted Edwards curve

$$(aX^2+Y^2)Z^2=Z^4+dX^2Y^2.$$

For $Z_1\neq 0$ the homogeneous point $(X_1:Y_1:Z_1)$ represents the affine point $(X_1/Z_1,Y_1/Z_1)$ on $\mathrm{E}_{\mathrm{E},a,d}$.

We checked the following explicit formulas for addition and doubling with the help of the Magma computer-algebra system, following the approach of the EFD [3].

5.3. Addition in projective coordinates. The following formulas compute $(X_3:Y_3:Z_3)=(X_1:Y_1:Z_1)+(X_2:Y_2:Z_2)$ in $10\mathbf{M}+1\mathbf{S}+2\mathbf{D}+7\mathbf{a}$, where the $2\mathbf{D}$ are one multiplication by a and one by d:

$$\begin{aligned}&A=Z_1\cdot Z_2;\ B=A^2;\ C=X_1\cdot X_2;\ D=Y_1\cdot Y_2;\ E=d\cdot C\cdot D;\\&F=B-E;\ G=B+E;\ X_3=A\cdot F\cdot((X_1+Y_1)\cdot(X_2+Y_2)-C-D);\\&Y_3=A\cdot G\cdot(D-a\cdot C);\ Z_3=F\cdot G.\end{aligned}$$

5.4. Doubling in projective coordinates. The following formulas compute $(X_3:Y_3:Z_3)=2(X_1:Y_1:Z_1)$ in $3\mathbf{M}+4\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, where the $1\mathbf{D}$ is a multiplication by a:

$$\begin{aligned}&B=(X_1+Y_1)^2;\ C=X_1^2;\ D=Y_1^2;\ E=a\cdot C;F:=E+D;\ H=Z_1^2;\\&J=F-2H;\ X_3=(B-C-D)\cdot J;\ Y_3=F\cdot(E-D);\ Z_3=F\cdot J.\end{aligned}$$

5.5. Clearing denominators in Edwards addition. Here is an alternative approach to arithmetic on the twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d}$ when a is a square in k.

The curve $\mathrm{E}_{\mathrm{E},a,d}:a\bar{x}^2+\bar{y}^2=1+d\bar{x}^2\bar{y}^2$ is isomorphic to the Edwards curve $\mathrm{E}_{\mathrm{E},1,d/a}:x^2+y^2=1+(d/a)x^2y^2$ by $x=\sqrt{a}\bar{x}$ and $y=\bar{y}$; see Section 2.4. The following formulas add on $\mathrm{E}_{\mathrm{E},1,d/a}$ using $10\mathbf{M}+1\mathbf{S}+3\mathbf{D}+7\mathbf{a}$, where the $3\mathbf{D}$ are two multiplications by a and one by d:

$$\begin{aligned}&A=Z_1\cdot Z_2;\ B=a\cdot A^2;\ H=a\cdot A;\ C=X_1\cdot X_2;\ D=Y_1\cdot Y_2;\ E=d\cdot C\cdot D;\\&F=B-E;\ G=B+E;\ X_3=H\cdot F\cdot((X_1+Y_1)\cdot(X_2+Y_2)-C-D);\\&Y_3=H\cdot G\cdot(D-C);\ Z_3=F\cdot G.\end{aligned}$$

One can double on $\mathrm{E}_{\mathrm{E},1,d/a}$ with $3\mathbf{M}+4\mathbf{S}+6\mathbf{a}$, independent of the curve coefficient d/a, using the formulas from [4, Section 4].

Our addition formulas for $\mathrm{E}_{\mathrm{E},1,d/a}$ are slower (by 1 multiplication by a) than our addition formulas for $\mathrm{E}_{\mathrm{E},a,d}$. On the other hand, doubling for $\mathrm{E}_{\mathrm{E},1,d/a}$ is faster (by 1 multiplication by a) than doubling for $\mathrm{E}_{\mathrm{E},a,d}$. Some applications (such as batch signature verification) have more additions than doublings, while other applications have more doublings than additions, so all of the formulas are of interest.

5.6. Inverted twisted Edwards coordinates. Another way to avoid inversions is to let a point $(X_1 : Y_1 : Z_1)$ on the curve

$$(X^2+aY^2)Z^2 = X^2Y^2+dZ^4$$

with $X_1Y_1Z_1 \neq 0$ correspond to the affine point $(Z_1/X_1, Z_1/Y_1)$ on $\mathrm{E}_{\mathrm{E},a,d}$.

Bernstein and Lange introduced these inverted coordinates in [5], for the case $a = 1$, and observed that the coordinates save time in addition. We generalize to arbitrary a.

5.7. Addition in inverted coordinates. The following formulas compute $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ in $9\mathbf{M}+1\mathbf{S}+2\mathbf{D}+7\mathbf{a}$, where the $2\mathbf{D}$ are one multiplication by a and one by d:

$$\begin{aligned}
&A = Z_1 \cdot Z_2;\ B = dA^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2;\ E = C \cdot D;\\
&H = C - aD;\ I = (X_1+Y_1)\cdot(X_2+Y_2) - C - D;\\
&X_3 = (E+B)\cdot H;\ Y_3 = (E-B)\cdot I;\ Z_3 = A \cdot H \cdot I.
\end{aligned}$$

5.8. Doubling in inverted coordinates. The following formulas compute $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ in $3\mathbf{M}+4\mathbf{S}+2\mathbf{D}+6\mathbf{a}$, where the $2\mathbf{D}$ are one multiplication by a and one by $2d$:

$$\begin{aligned}
&A = X_1^2;\ B = Y_1^2;\ U = aB;\ C = A+U;\ D = A-U;\\
&E = (X_1+Y_1)^2 - A - B;\ X_3 = C \cdot D;\ Y_3 = E \cdot (C - 2d \cdot Z_1^2);\ Z_3 = D \cdot E.
\end{aligned}$$

6 Edwards versus twisted Edwards

We introduced twisted Edwards curves as a generalization of Edwards curves. Is this generalization actually useful for cryptographic purposes?

Section 4 showed that, over prime fields $\mathbf{F}_p$ where $p \equiv 1 \pmod 4$, twisted Edwards curves cover considerably more elliptic curves than Edwards curves do. In particular, for "4 times odd" elliptic curves over such prime fields, the coverage of Edwards curves is only about 60% of the coverage of twisted Edwards curves. One can choose a to be very small, making twisted Edwards curves essentially as fast as Edwards curves and thus bringing the speed of the Edwards addition law to a wider variety of elliptic curves.

Even when a elliptic curve *can* be expressed in Edwards form, expressing the same curve in twisted Edwards form often saves time in arithmetic. In this section we review the issues faced by implementors aiming for top speed. We give examples of the impact of twisted Edwards curves for implementors who are faced with externally specified curves, and for implementors who are free to choose their own curves.

6.1. How twisting can save time. The following table summarizes the speeds of addition and doubling in standard (projective) coordinates on Edwards curves, standard coordinates on twisted Edwards curves, inverted coordinates on Edwards curves, and inverted coordinates on twisted Edwards curves:

Type	Source of algorithms	Addition	Doubling
Edwards	[4, Section 4]	10**M**+1**S**+1**D**	3**M**+4**S**
Twisted Edwards	this paper	10**M**+1**S**+2**D**	3**M**+4**S**+1**D**
Inverted Edwards	[5, Sections 4–5]	9**M**+1**S**+1**D**	3**M**+4**S**+1**D**
Inverted twisted Edwards	this paper	9**M**+1**S**+2**D**	3**M**+4**S**+2**D**

If a curve E is expressible as an Edwards curve, is there any reason to consider more general expressions of E as a twisted Edwards curve? One might think, from a glance at the above table, that the answer is no: twisting appears to lose 1**D** in every coordinate system and for every group operation without gaining anything. However, there are many situations where the answer is yes!

Specifically, instead of performing computations on the Edwards curve $\mathrm{E}_{\mathrm{E},1,\bar{d}}$ over $\mathbf{F}_p$, one can perform computations on the twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d}$ over $\mathbf{F}_p$ for any (a, d) such that $\bar{d} = d/a$ and such that a is a square in $\mathbf{F}_p$. (It is convenient for computing the isomorphism, but certainly not essential, for a to be the square of a small integer.) In particular, many curves have $\bar{d}$ expressible as a ratio d/a where both d and a are small, much smaller than any integer congruent to $\bar{d}$ modulo p. In the non-twisted Edwards case the 1**D** in the table above is a multiplication by $\bar{d}$ while the 2**D** in the twisted Edwards case are one multiplication by d and one multiplication by a, often taking *less* time than a multiplication by $\bar{d}$.

Consider, for example, the curve "Curve25519" used in [1] to set speed records for elliptic-curve Diffie-Hellman before the advent of Edwards curves. Curve25519 is a particular elliptic curve over $\mathbf{F}_p$ where $p = 2^{255} - 19$. Bernstein and Lange point out in [4, Section 2] that Curve25519 can be expressed as an Edwards curve $x^2 + y^2 = 1 + (121665/121666)x^2y^2$. We point out that this curve is isomorphic to the twisted Edwards curve $121666x^2 + y^2 = 1 + 121665x^2y^2$, and that the twisted Edwards curve provides faster arithmetic. Each addition on the twisted Edwards curve involves only one multiplication by 121665 and one multiplication by 121666.

The decision between Edwards curves and twisted Edwards curves interacts with the decision between standard Edwards coordinates and inverted Edwards coordinates. Frequent additions make inverted Edwards coordinates more impressive; large a, d make inverted Edwards coordinates less impressive.

6.2. Choosing twisted Edwards curves. Often implementors are free to choose their own curves for the best possible speed. To illustrate the benefits of this flexibility we studied "small" twisted Edwards curves modulo several primes of cryptographic size: $2^{160} - 47$, the largest prime below 2^{160}; $2^{192} - 2^{64} - 1$, the prime used for NIST's P-192 elliptic curve; $2^{224} - 2^{96} + 1$, the prime used for NIST's P-224 elliptic curve; and $2^{255} - 19$, the prime used in [1]. Specifically, we enumerated twisted Edwards curves $\mathrm{E}_{\mathrm{E},a,d}$ for thousands of small pairs (a, d), and we checked which curves had small cofactors over $\mathbf{F}_p$, i.e., had group orders $h \cdot$prime where the cofactor h is small. We give some examples of twisted Edwards curves with small cofactor, tiny a, and tiny d, supporting exceptionally fast arithmetic.

For $p = 2^{192} - 2^{64} - 1$, the twisted Edwards curve $\mathrm{E}_{\mathrm{E},102,47} : 102x^2 + y^2 = 1 + 47x^2y^2$ has cofactor 4. Arithmetic on $\mathrm{E}_{\mathrm{E},102,47}$ is impressively fast, and the cofactor is minimal. The nontrivial quadratic twist $\mathrm{E}_{\mathrm{E},1122,517}$ has cofactor only 28, protecting against the active attacks discussed in (e.g.) [1, Section 3].

For $p = 2^{224} - 2^{96} + 1$, the twisted Edwards curve $\mathrm{E}_{\mathrm{E},12,1}$ has cofactor 3456, and its nontrivial quadratic twist $\mathrm{E}_{\mathrm{E},132,11}$ has cofactor 20. The coefficients $a = 12$ and $d = 1$ here are spectacularly small. The cofactor 3456 is not minimal but can still be considered for cryptographic purposes.

If active attacks are stopped in other ways then one can find even smaller pairs (a, d). For $p = 2^{160} - 47$ the twisted Edwards curve $\mathrm{E}_{\mathrm{E},23,-6}$ has cofactor 4; for comparison, the first Edwards curve we found with small parameters a and d and with cofactor 4 over the same field was $\mathrm{E}_{\mathrm{E},1,268}$. For $p = 2^{255} - 19$ the twisted Edwards curve $\mathrm{E}_{\mathrm{E},29,-28}$ has cofactor 4 and the twisted Edwards curve $\mathrm{E}_{\mathrm{E},25,2}$ has cofactor 8.

References

1. Daniel J. Bernstein, *Curve25519: new Diffie-Hellman speed records*, in [13] (2006), 207–228. URL: `http://cr.yp.to/papers.html#curve25519`. Citations in this document: §6.1, §6.2, §6.2.
2. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *ECM using Edwards curves* (2007). Citations in this document: §1.
3. Daniel J. Bernstein, Tanja Lange, *Explicit-formulas database* (2007). URL: `http://hyperelliptic.org/EFD`. Citations in this document: §5.2.
4. Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in [10] (2007), 29–50. URL: `http://cr.yp.to/papers.html#newelliptic`. Citations in this document: §1, §1, §2, §2.1, §2.4, §3.4, §3.4, §3.4, §3.4, §3.4, §3.4, §4.1, §5.1, §5.1, §5.5, §6.1, §6.1.
5. Daniel J. Bernstein, Tanja Lange, *Inverted Edwards coordinates*, in [6] (2007), 20–27. URL: `http://cr.yp.to/papers.html#inverted`. Citations in this document: §1, §5.6, §6.1.
6. Serdar Boztas, Hsiao-Feng Lu (editors), *Applied algebra, algebraic algorithms and error-correcting codes*, Lecture Notes in Computer Science, 4851, Springer, 2007. See [5].
7. Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422. URL: `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`. Citations in this document: §1.

8. Steven D. Galbraith, James McKee, *The probability that the number of points on an elliptic curve over a finite field is prime*, Journal of the London Mathematical Society **62** (2000), 671–684. URL: `http://www.isg.rhul.ac.uk/~sdg/pubs.html`. Citations in this document: §4, §4.1.
9. Hideki Imai, Yuliang Zheng (editors), *Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18–20, 2000, Proceedings*, Lecture Notes in Computer Science, 1751, Springer, 2000. ISBN 978–3–540–66967–8. See [12].
10. Kaoru Kurosawa (editor), *Advances in cryptology — ASIACRYPT 2007*, Lecture Notes in Computer Science, 4833, Springer, 2007. See [4].
11. Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264. ISSN 0025–5718. MR 88e:11130. URL: `http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3`. Citations in this document: §3.4.
12. Katsuyuki Okeya, Hiroyuki Kurumatani, Kouichi Sakurai, *Elliptic curves with the Montgomery-form and their cryptographic applications*, in [9] (2000), 238–257. Citations in this document: §3.4, §3.4.
13. Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin (editors), *9th international conference on theory and practice in public-key cryptography, New York, NY, USA, April 24–26, 2006, proceedings*, Lecture Notes in Computer Science, 3958, Springer, Berlin, 2006. ISBN 978–3–540–33851–2. See [1].