Inverted Edwards coordinates

Inverted Edwards Coordinates

Daniel J. Bernstein[1] and Tanja Lange[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
tanja@hyperelliptic.org

Abstract. Edwards curves have attracted great interest for several reasons. When curve parameters are chosen properly, the addition formulas use only $10\mathbf{M} + 1\mathbf{S}$. The formulas are *strongly unified*, i.e., work without change for doublings; even better, they are *complete*, i.e., work without change for all inputs. Dedicated doubling formulas use only $3\mathbf{M} + 4\mathbf{S}$, and dedicated tripling formulas use only $9\mathbf{M} + 4\mathbf{S}$.

This paper introduces *inverted Edwards coordinates*. Inverted Edwards coordinates $(X_1 : Y_1 : Z_1)$ represent the affine point $(Z_1/X_1, Z_1/Y_1)$ on an Edwards curve; for comparison, standard Edwards coordinates $(X_1 : Y_1 : Z_1)$ represent the affine point $(X_1/Z_1, Y_1/Z_1)$.

This paper presents addition formulas for inverted Edwards coordinates using only $9\mathbf{M} + 1\mathbf{S}$. The formulas are not complete but still are strongly unified. Dedicated doubling formulas use only $3\mathbf{M} + 4\mathbf{S}$, and dedicated tripling formulas use only $9\mathbf{M} + 4\mathbf{S}$. Inverted Edwards coordinates thus save $1\mathbf{M}$ for each addition, without slowing down doubling or tripling.

Keywords: Elliptic curves, addition, doubling, explicit formulas, Edwards coordinates, inverted Edwards coordinates, side-channel countermeasures, unified addition formulas, strongly unified addition formulas.

1 Introduction

In [8] Edwards proposed a new normal form for elliptic curves and gave an addition law that is remarkably symmetric in the x and y coordinates. In [4], using coordinates $(X : Y : Z)$ to represent the point $(X/Z, Y/Z)$ on an Edwards curve, we showed that curve addition could be performed using only $10\mathbf{M} + 1\mathbf{S}$ (i.e., 11 field multiplications, of which 1 is a squaring) and that curve doubling could be performed using only $3\mathbf{M} + 4\mathbf{S}$. We presented a comprehensive survey

⋆ Permanent ID of this document: 0ef034ea1cdbb58a5182aaaefbea6754. Date of this document: 2007.10.03. This work has been supported in part by the European Commission through the IST Programme under Contract IST–2002–507932 ECRYPT. This work was carried out while the first author was visiting Technische Universiteit Eindhoven.

S. Boztaş and H.F. Lu (Eds.): AAECC 2007, LNCS 4851, pp. 20–27, 2007.

of speeds of our formulas and previous formulas for elliptic-curve arithmetic in various representations. The survey showed that Edwards curves provide the fastest additions and almost the fastest doublings. The only faster doublings were from doubling-oriented Doche/Icart/Kohel curves, which come with rather inefficient addition formulas.

One of the attractive features of the Edwards addition law is that it is *strongly unified*: the addition law works without change for doublings. We showed in [4] that, when curve parameters are chosen properly, the addition law is even *complete*: it works for all inputs, with no exceptional cases. Our fast addition formulas in [4] have the same features. See Section 2 of this paper for a more detailed review of Edwards curves.

In [2], together with Birkner and Peters, we showed that tripling on Edwards curves could be performed using only $9\mathbf{M} + 4\mathbf{S}$. We also analyzed the optimal combinations of additions, doublings, triplings, windowing methods, on-the-fly precomputations, curve shapes, and curve formulas, improving upon the analysis in [6] by Doche and Imbert. Hisil, Carter, and Dawson independently developed essentially the same tripling formulas; see [9].

New Contributions. This paper presents an even faster coordinate system for elliptic curves: namely, *inverted Edwards coordinates*, using coordinates $(X : Y : Z)$ to represent the point $(Z/X, Z/Y)$ on an Edwards curve. In Section 4 we present formulas for curve addition in inverted Edwards coordinates using only $9\mathbf{M} + 1\mathbf{S}$, saving $1\mathbf{M}$ compared to standard Edwards coordinates.

Inverted Edwards coordinates, unlike standard Edwards coordinates, do not have complete addition formulas: some points, such as the neutral element, must be handled separately. But our addition formulas still have the advantage of strong unification: they can be used without change to double a point.

In Sections 5 and 6 we present formulas for doubling and tripling in inverted Edwards coordinates using only $3\mathbf{M} + 4\mathbf{S}$ and $9\mathbf{M} + 4\mathbf{S}$, matching the speeds of standard Edwards coordinates.

All of the operation counts stated above assume small curve parameters and disregard the cost of multiplying by a curve parameter. Arbitrary curve parameters cost $1\mathbf{M}$ extra for each addition, each doubling, and each tripling. The penalty for standard Edwards coordinates is smaller: arbitrary curve parameters cost $1\mathbf{M}$ extra for addition but nothing for doubling or tripling.

In Section 7 we revisit the comparison from [4], analyzing the impact of inverted Edwards coordinates and other recent speedups.

2 Review of Edwards Curves

Let k be a field. Throughout this paper we assume that $2 \neq 0$ in k.

A curve in *Edwards form* is given by an equation

$$x^2 + y^2 = 1 + dx^2y^2,$$

where $d \notin \{0, 1\}$. Every Edwards curve is birationally equivalent to an elliptic curve in Weierstrass form. See [4, Section 3] for an explicit description of the equivalence.

One reason for the great interest in Edwards curves is that the Edwards addition law

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

is *strongly unified*: it applies to doubling as well as to general addition, unlike the usual Weierstrass addition law. Strongly unified addition formulas had previously been published for Jacobi intersections, Jacobi quartics, and Weierstrass curves in projective coordinates, but the Edwards formulas are considerably faster.

We showed in [4, Theorem 3.3] that if d is not a square in k then the Edwards addition law has an even more attractive feature: it is *complete*. This means that there are no points $(x_1, y_1), (x_2, y_2)$ on the curve where the denominators vanish; the Edwards addition law produces the correct output for *every* pair of input points. The neutral element $(0, 1)$ does not cause any trouble. The Edwards curve has two singularities at infinity, corresponding to four points on the desingularization of the curve; but those four points are defined over $k(\sqrt{d})$, not over k.

To the best of our knowledge, the Edwards addition law is the only complete addition law stated in the literature. Previous addition laws have exceptional cases and require careful handling by the implementor to avoid the risk of incorrect results and to avoid the risk of leaking secret information through side channels. It should be possible to build a complete addition law for some Weierstrass curves starting from the formulas in [5], but we would not expect the resulting law to be nearly as fast as the Edwards addition law.

In [4] we suggested using homogeneous coordinates $(X_1 : Y_1 : Z_1)$, where $(X_1^2 + Y_1^2)Z_1^2 = Z_1^4 + dX_1^2 Y_1^2$ and $Z_1 \neq 0$, to represent the point $(X_1/Z_1, Y_1/Z_1)$ on the Edwards curve. Here $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for any $\lambda \neq 0$. In [4, Section 4] we presented explicit formulas for addition in this representation using $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, where $\mathbf{M}$ denotes the cost of a field multiplication, $\mathbf{S}$ the cost of a field squaring, $\mathbf{D}$ the cost of a multiplication by the curve parameter d, and $\mathbf{a}$ the cost of a field addition.

Implementations can gain speed, at the expense of simplicity, by using dedicated doubling formulas for additions where the inputs are known to be equal. In [4, Section 4] we presented explicit doubling formulas using $3\mathbf{M} + 4\mathbf{S} + 6\mathbf{a}$. Completeness remains beneficial in this situation: one does not need to check for other exceptions if the curve parameter d is not a square.

3 Inverted Edwards Coordinates

In this and the following sections we consider a different representation of points on an Edwards curve $x^2 + y^2 = 1 + dx^2 y^2$. We use three coordinates $(X_1 : Y_1 : Z_1)$, where

$$(X_1^2 + Y_1^2)Z_1^2 = X_1^2 Y_1^2 + dZ_1^4$$

and $X_1Y_1Z_1 \neq 0$, to represent the point $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve. We refer to these coordinates as *inverted Edwards coordinates*. As before, $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for any $\lambda \neq 0$.

It is easy to convert from standard Edwards coordinates $(X_1 : Y_1 : Z_1)$ to inverted Edwards coordinates: simply compute $(Y_1Z_1 : X_1Z_1 : X_1Y_1)$ with three multiplications. The same computation also performs the opposite conversion from inverted Edwards coordinates to standard Edwards coordinates.

For computations we use the vector (X_1, Y_1, Z_1) to represent the point $(X_1 : Y_1 : Z_1)$ in inverted Edwards coordinates.

Special points. The requirement $X_1Y_1Z_1 \neq 0$ means that inverted Edwards coordinates cannot represent points (x_1, y_1) on the Edwards curve that satisfy $x_1y_1 = 0$. There are four such points: the neutral element $(0, 1)$, the point $(0, -1)$ of order 2, and the points $(\pm 1, 0)$ of order 4. Additions that involve these points as inputs or outputs must be handled by separate routines.

The four points $(0, 1), (0, -1), (1, 0), (-1, 0)$ are $(0 : 1 : 1), (0 : -1 : 1)$, $(1 : 0 : 1), (-1 : 0 : 1)$ in standard Edwards coordinates. Applying the aforementioned conversion to inverted Edwards coordinates, and ignoring the requirement $X_1Y_1Z_1 \neq 0$, produces points at infinity on the projective curve $(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4$: specifically, $(1 : 0 : 0), (-1 : 0 : 0), (0 : 1 : 0), (0 : -1 : 0)$. But then the rule $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ equates $(1 : 0 : 0)$ with $(-1 : 0 : 0)$, losing the distinction between $(0, 1)$ and $(0, -1)$, and similarly losing the distinction between $(1, 0)$ and $(-1, 0)$.

To have unique representations for the computations it is convenient to use the vectors $(1, 0, 0), (-1, 0, 0), (0, -1, 0), (0, 1, 0)$ to represent $(0, 1), (0, -1), (1, 0)$, $(-1, 0)$. Note that these representations are *not* homogeneous and that for algorithmic reasons $(\pm 1, 0)$ correspond to $(0, \mp 1, 0)$. One must be careful to check for $Z_1 = 0$ before adding $(X_1 : Y_1 : Z_1)$ to another point, and to check for $X_1Y_1 = 0$ before applying the conversions to and from standard Edwards coordinates.

In many applications one restricts attention to a subgroup of odd order, so the only special point is the neutral element and fewer checks are required. One can also randomize computations so that special points have a negligible chance of occurring; see [4, Section 8] for pointers to the literature.

Geometry. Recall that the desingularization of an Edwards curve has, over $k(\sqrt{d})$, four points that map to the two singularities at infinity on the curve. It also has four points that map without ramification to $(0, 1)$, $(0, -1)$, $(1, 0)$, and $(-1, 0)$.

Mapping the same desingularization to the projective curve $(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4$ takes the first four points without ramification to $(0 : \pm\sqrt{d} : 1)$ and $(\pm\sqrt{d} : 0 : 1)$, and takes the second four points to two singularities at infinity.

When d is not a square, the first map has no ramification points over k and allows a complete addition law on the Edwards curve. The second map always has ramification points, and in particular is ramified at the neutral element.

For mathematicians it is perhaps more satisfying to start from the projective curve $(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4$ and define an addition law on it, including

the points $(0 : \pm\sqrt{d} : 1)$ and $(\pm\sqrt{d} : 0 : 1)$, without mapping to an Edwards curve. We restricted to points $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ to maintain the link with Edwards curves and the Edwards addition law.

4 Addition

Obtaining more efficient addition formulas was our main goal in investigating inverted Edwards coordinates. Inspecting the addition formulas in [4, Section 4] one notices that the computations of the resulting X_3 and Y_3 each involve a multiplication by Z_1Z_2.

Inserting Z_i/X_i for x_i and Z_i/Y_i for y_i in the Edwards addition law (assuming $X_iY_iZ_i \neq 0$) we obtain

$$\left(\frac{Z_1}{X_1},\frac{Z_1}{Y_1}\right)+\left(\frac{Z_2}{X_2},\frac{Z_2}{Y_2}\right)=\left(\frac{(X_2Y_1+X_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2+dZ_1^2Z_2^2},\frac{(X_1X_2-Y_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2-dZ_1^2Z_2^2}\right)=\left(\frac{Z_3}{X_3},\frac{Z_3}{Y_3}\right)$$

where

$$\begin{aligned} X_3 &= (X_1X_2 - Y_1Y_2)(X_1X_2Y_1Y_2 + dZ_1^2Z_2^2) \\ Y_3 &= (X_2Y_1 + X_1Y_2)(X_1X_2Y_1Y_2 - dZ_1^2Z_2^2) \\ Z_3 &= (X_1X_2 - Y_1Y_2)(X_2Y_1 + X_1Y_2)Z_1Z_2. \end{aligned}$$

This shows the idea behind inverted Edwards coordinates, namely that in this representation only Z_3 needs to be multiplied with Z_1Z_2, which saves $1\mathbf{M}$ in total. Compared to the addition in Edwards coordinates the degree of these formulas is only 6 as opposed to 8 in that representation.

We then eliminate multiplications from these formulas, as in [4, Section 4], obtaining the following formulas to compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ in inverted Edwards coordinates, given $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$:

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

One readily counts $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, as advertised in the introduction. We have added these formulas to the EFD [3] for formal verification that the results coincide with the original Edwards addition law and that the formulas are strongly unified.

Restricted additions. *Mixed addition* means that Z_2 is known to be 1. There is an obvious saving of $1\mathbf{M}$ in this case since $A = Z_1 \cdot Z_2 = Z_1$, leading to a total cost of $8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$.

Readdition means that $(X_2 : Y_2 : Z_2)$ has been added to another point before. This means that computations depending only on $(X_2 : Y_2 : Z_2)$, such as X_2+Y_2,

can be cached from the previous addition. We have not found a way to save **M** or **S** in this case.

Special points. The above description of addition ignored the possibility of the special points $(0,1),(0,-1),(1,0),(-1,0)$ appearing as summands or as the sum. We now deal with that possibility. We represent these points as the vectors $(1,0,0),(-1,0,0),(0,-1,0),(0,1,0)$ respectively, as discussed in Section 3. We assume that d is not a square.

Special points as summands are easy to handle. If $Z_1 = 0$ or $Z_2 = 0$ then the sum of (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) is $(X_1X_2 - Y_1Y_2, X_2Y_1 + X_1Y_2, Z_1 + Z_2)$.

Even if neither summand is a special point, the sum could be a special point. If $I = 0$ and $Y_2Z_1 = Y_1Z_2$ then the sum is $(1,0,0)$. If $I = 0$ and $Y_2Z_1 = -Y_1Z_2$ then the sum is $(-1,0,0)$. If $H = 0$ and $Y_2Z_1 = -X_1Z_2$ then the sum is $(0,1,0)$. If $H = 0$ and $Y_2Z_1 = X_1Z_2$ then the sum is $(0,-1,0)$.

To derive these output rules, observe that two points (x_1, y_1) and (x_2, y_2) on the Edwards curve have sum $(0,1)$ if and only if $(x_2, y_2) = (-x_1, y_1)$. In this case $(Z_2/X_2, Z_2/Y_2) = (-Z_1/X_1, Z_1/Y_1)$ so, in the notation of our explicit formulas, $I = X_1Y_2 + Y_1X_2 = X_1Y_1Z_2/Z_1 - Y_1X_1Z_2/Z_1 = 0$ and $Y_2Z_1 = Y_1Z_2$. Similarly, two points (x_1, y_1) and (x_2, y_2) having sum $(0,-1)$ end up with $I = 0$ but with $Y_2Z_1 = -Y_1Z_2$; two points (x_1, y_1) and (x_2, y_2) having sum $(1,0)$ end up with $H = 0$ and $Y_2Z_1 = X_1Z_2$; two points (x_1, y_1) and (x_2, y_2) having sum $(-1,0)$ end up with $H = 0$ but with $Y_2Z_1 = -X_1Z_2$.

To see that the output rules are exclusive, suppose that $H = 0$ and $I = 0$. Then $X_1X_2 = Y_1Y_2$ and $X_1Y_2 + X_2Y_1 = 0$, so $X_1^2X_2 = X_1Y_1Y_2$ and $X_1Y_1Y_2 + X_2Y_1^2 = 0$, so $(X_1^2 + Y_1^2)X_2 = 0$; all variables are nonzero, so $X_1^2 + Y_1^2 = 0$. The curve equation $(X_1^2 + Y_1^2)Z_1^2 = X_1^2Y_1^2 + dZ_1^4$ now implies $0 = X_1^2(-X_1^2) + dZ_1^4$; i.e., $d = (X_1/Z_1)^4$, contradicting the assumption that d is not a square.

5 Doubling

Doubling refers to the case that the inputs $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are known to be equal. If $X_1Y_1Z_1 = 0$ the special formulas from Section 4 apply. Otherwise inserting Z_1/X_1 for x_1 and x_2 and Z_1/Y_1 for y_1 and y_2 in the Edwards addition law we obtain

$$2(x_1, y_1) = \left(\frac{2X_1Y_1Z_1^2}{X_1^2Y_1^2 + dZ_1^4}, \frac{(X_1^2 - Y_1^2)Z_1^2}{X_1^2Y_1^2 - dZ_1^4}\right) = \left(\frac{2X_1Y_1}{X_1^2 + Y_1^2}, \frac{X_1^2 - Y_1^2}{X_1^2 + Y_1^2 - 2dZ_1^2}\right).$$

In the second equality we have used the curve equation to replace $X_1^2Y_1^2$ by $(X_1^2 + Y_1^2)Z_1^2 - dZ_1^4$, and then cancelled Z_1^2, reducing the overall degree of the formulas to 4. The resulting coordinates are

$$\begin{aligned} X_3 &= (X_1^2 + Y_1^2)(X_1^2 - Y_1^2) \\ Y_3 &= 2X_1Y_1(X_1^2 + Y_1^2 - 2dZ_1^2) \\ Z_3 &= 2X_1Y_1(X_1^2 - Y_1^2). \end{aligned}$$

The explicit formulas in this case need $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D} + 6\mathbf{a}$:

$$A = X_1^2;\ B = Y_1^2;\ C = A + B;\ D = A - B;\ E = (X_1 + Y_1)^2 - C;$$
$$Z_3 = D \cdot E;\ X_3 = C \cdot D;\ Y_3 = E \cdot (C - 2d \cdot Z_1^2).$$

6 Tripling

In Edwards coordinates tripling ($9\mathbf{M} + 4\mathbf{S} + 8\mathbf{a}$, or alternatively $7\mathbf{M} + 7\mathbf{S} + 16\mathbf{a}$) is faster than the sequential computation of a doubling ($3\mathbf{M} + 4\mathbf{S} + 6\mathbf{a}$) followed by an addition ($10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$). The main speedup comes from using the curve equation to reduce the degree of the tripling formulas. See Section 1 for credits and references.

For inverted Edwards coordinates with $X_1Y_1Z_1 \neq 0$ we now provide two sets of tripling formulas. Both sets have been added to the EFD [3] for formal verification. The first set needs $9\mathbf{M} + 4\mathbf{S} + 1\mathbf{D} + 10\mathbf{a}$:

$$A = X_1^2;\ B = Y_1^2;\ C = Z_1^2;\ D = A + B;\ E = 4(D - d \cdot C);$$
$$H = 2D \cdot (B - A);\ P = D^2 - A \cdot E;\ Q = D^2 - B \cdot E;$$
$$X_3 = (H + Q) \cdot Q \cdot X_1;\ Y_3 = (H - P) \cdot P \cdot Y_1;\ Z_3 = P \cdot Q \cdot Z_1.$$

The second set needs $7\mathbf{M} + 7\mathbf{S} + 1\mathbf{D} + 17\mathbf{a}$:

$$A = X_1^2;\ B = Y_1^2;\ C = Z_1^2;\ D = A + B;\ E = 4(D - d \cdot C);$$
$$H = 2D \cdot (B - A);\ P = D^2 - A \cdot E;\ Q = D^2 - B \cdot E;$$
$$X_3 = (H + Q) \cdot ((Q + X_1)^2 - Q^2 - A);\ Y_3 = 2(H - P) \cdot P \cdot Y_1;$$
$$Z_3 = P \cdot ((Q + Z_1)^2 - Q^2 - C).$$

The second set is faster if $\mathbf{S}/\mathbf{M}$ is small.

Triplings, like doublings, have similar speeds for inverted Edwards coordinates and standard Edwards coordinates. Inverted Edwards coordinates speed up addition by reducing the degree of the formulas, but the curve equation already appears to have produced the minimal degrees for doublings and triplings, so the lack of further improvements does not come as a surprise.

Special points. Tripling special points is very easy: $3(X_1, Y_1, 0) = (X_1, -Y_1, 0)$.

7 Comparison

The EFD [3] is meant to provide an up-to-date database with all curve forms and coordinate systems ever proposed. A comparison in a paper can only give a snapshot of what is known today. Most of the conclusions in [4] remain unchanged, but science has developed even in the short time since then!

Duquesne in [7] proposed what we call "extended Jacobi-quartic coordinates," now described in detail in the EFD. Duquesne's addition formulas use

$9\mathbf{M}+2\mathbf{S}+1\mathbf{D}$, saving $1\mathbf{M}-1\mathbf{S}$ compared to standard Edwards coordinates. These addition formulas are strongly unified but not complete: they can be used for doublings but have some exceptional cases. In the EFD we improve Duquesne's formulas to use $8\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$, saving another $1\mathbf{M} - 1\mathbf{S}$.

Hisil, Carter, and Dawson in [9] improved various elliptic-curve addition formulas, and in particular gave doubling formulas for extended Jacobi-quartic coordinates using $3\mathbf{M} + 4\mathbf{S}$. This is as fast as doubling in standard Edwards coordinates.

However, addition in inverted Edwards coordinates is even faster, saving an additional $2\mathbf{S}-1\mathbf{M}$, and has just as fast doublings (for small d). Inverted Edwards coordinates have the same advantage of being strongly unified.

The comparisons of different coordinate systems for scalar multiplications using DBNS in [2] have been updated to include the speeds of [7] and [9], and to include inverted Edwards coordinates. The comparison shows that, out of currently known methods for scalar multiplication on elliptic curves, inverted Edwards coordinates (with very few triplings) are the fastest.

To conclude we summarize the current situation: Edwards coordinates offer the only complete addition law stated in the literature. If completeness is not required then inverted Edwards coordinates are the new speed leader.

References

1. Barua, R., Lange, T. (eds.): INDOCRYPT 2006. LNCS, vol. 4329. Springer, Heidelberg (2006)
2. Bernstein, D.J., Birkner, P., Lange, T., Peters, C.: Optimizing Double-Base Elliptic-Curve Single-Scalar Multiplication. In: Srinathan, K., Pandu Rangan, C., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 167–182. Springer, Heidelberg (2007)
3. Bernstein, D.J., Lange, T.: Explicit-Formulas Database, `http://www.hyperelliptic.org/EFD`
4. Bernstein, D.J., Lange, T.: Faster Addition and Doubling on Elliptic Curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007), `http://cr.yp.to/newelliptic/`
5. Bosma, W., Lenstra Jr., H.W.: Complete Systems of Two Addition Laws for Elliptic Curves. J. Number Theory 53, 229–240 (1995)
6. Doche, C., Imbert, L.: Extended Double-Base Number System with Applications to Elliptic Curve Cryptography. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 335–348. Springer, Heidelberg (2006)
7. Duquesne, S.: Improving the Arithmetic of Elliptic Curves in the Jacobi Model. Information Processing Letters 104, 101–105 (2007)
8. Edwards, H.M.: A Normal Form for Elliptic Curves. Bulletin of the American Mathematical Society 44, 393–422 (2007), `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`
9. Hisil, H., Carter, G., Dawson, E.: New Formulae for Efficient Elliptic Curve Arithmetic. In: Srinathan, K., Pandu Rangan, C., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, Springer, Heidelberg (2007)
10. Kurosawa, K. (ed.): ASIACRYPT 2007. LNCS, vol. 4833. Springer, Heidelberg (2007)