# Differential Addition in generalized Edwards Coordinates

Benjamin Justus and Daniel Loebenberger

Bonn-Aachen International Center for Information Technology
Universität Bonn
53113 Bonn
Germany

**Abstract.** We use two parametrizations of points on elliptic curves in generalized Edwards form $x^2 + y^2 = c^2(1 + dx^2y^2)$ that omit the $x$-coordinate. The first parametrization leads to a differential addition formula that can be computed using $6\mathbf{M} + 4\mathbf{S}$, a doubling formula using $1\mathbf{M} + 4\mathbf{S}$ and a tripling formula using $4\mathbf{M} + 7\mathbf{S}$. The second one yields a differential addition formula that can be computed using $5\mathbf{M} + 2\mathbf{S}$ and a doubling formula using $5\mathbf{S}$. All formulas apply also for the case $c \neq 1$ and arbitrary curve parameter $d$. This generalizes formulas from the literature for the special case $c = 1$.
For both parametrizations the formula for recovering the missing $X$-coordinate is also provided.
**Keywords.** Elliptic curve, Edwards form, addition formula, differential addition

## 1 Introduction

Efficient arithmetic (addition, doubling and scalar multiplication) on elliptic curves is *the* core requirement of elliptic curve cryptography. It is the cornerstone in applications such as the digital signature algorithm (DSA), see [10], and Lenstra's elliptic curve factoring method [11]. Various ways of representing elliptic curves have been proposed for the purpose of efficient arithmetic. For an overview, the reader can consult the standard reference [7] or the online Explicit-Formulas Database (EFD)[1]. We have selected some of the top candidates and summarized them in the table below. Here $\mathbf{M}$ (resp. $\mathbf{S}$) refers to multiplication (resp. a squaring) in the field. We ignore in this paper multiplications by a constant and the additions in the field, since their cost is negligible when compared to the cost of multiplication or squaring.

With the advent of Edwards coordinates [8], extensive recent work [1–4] has provided formulas for addition on Edwards form that are more efficient (by a constant factor) than what is known for other representations. This makes the Edwards form particularly interesting for cryptographic applications.

[1] see `http://www.hyperelliptic.org/EFD`

Castryck, Galbraith and Farashahi [6] present doubling formulas for Edwards form with $c = 1$ like the one given in Corollary 1. They do not consider the case $c \neq 1$ and do not provide a general (differential) addition formula.

Gaudry and Lubicz [9] present general efficient algorithms for a much broader class of curves. In order to adapt their ideas to the context of elliptic curves in generalized Edwards form, one needs to explicitly express the group law in terms of Riemann's $\vartheta$ functions. Due to our inability to do so, we derive in this work formulas for elliptic curves in generalized Edwards form directly. We are in good company here; Castryck, Galbraith and Farashahi write: "This is an euphemistic rephrasing of our ignorance about Gaudry and Lubicz' result, which is somewhat hidden in a different framework."

Special cases of our result can also be found on EFD: There are several formulas given for $c = 1$ under the assumption that the curve parameter $d$ is a square in the field. This restriction on the curve parameter $d$ is annoying in practice, as the group law on elliptic curves in Edwards form is not complete anymore if $d$ is a square in the field. The formulas on EFD are on one hand consequences of [9] but can also be deduced from our general formulas in Theorem 1 and Corollary 1, as explained at the end of section 3.

**Table 1.** Some coordinate choices with fast arithmetic

| Forms | Coordinates | Addition Cost | Doubling Cost |
|---|---|---|---|
| Short Weierstraß | $(X : Y : Z) = (X/Z^2, Y/Z^3)$ | $12\mathbf{M} + 4\mathbf{S}$ | $4\mathbf{M} + 5\mathbf{S}$ |
| Montgomery form | $(X : Z)$ | $4\mathbf{M} + 1\mathbf{S}$ | $2\mathbf{M} + 3\mathbf{S}$ |
| Edwards form | $(X : Y : Z)$ | $10\mathbf{M} + 1\mathbf{S}$ | $3\mathbf{M} + 4\mathbf{S}$ |
| Inverted Edwards | $(X : Y : Z) = (Z/X, Z/Y)$ | $9\mathbf{M} + 1\mathbf{S}$ | $3\mathbf{M} + 4\mathbf{S}$ |
| Differential Edwards | $(Y : Z)$ | $4\mathbf{M} + 4\mathbf{S}$ | $4\mathbf{S}$ |
| ($c = 1$ and $d$ square) | | | |
| | $(Y^2 : Z^2)$ | $4\mathbf{M} + 2\mathbf{S}$ | $4\mathbf{S}$ |

In this work, we use two parametrizations for elliptic curves in generalized Edwards form to obtain efficient arithmetic: In the first parametrization a point on the curve is represented by the projective coordinate $(Y : Z)$. Notice that the $X$-coordinate is absent, so we cannot distinguish $P$ from $-P$. This is indeed similar to Montgomery's approach [12], where he represents a point in Weierstraß-coordinates by omitting the $Y$-coordinate. The parametrization used here leads to a differential addition formula, a doubling formula and a tripling formula on elliptic curves in generalized Edwards form. The addition formula can be computed using $6\mathbf{M} + 4\mathbf{S}$ ($5\mathbf{M} + 4\mathbf{S}$ in the case $c = 1$), the doubling formula using $1\mathbf{M} + 4\mathbf{S}$ ($5\mathbf{S}$ when $c = 1$) and the tripling formula using $4\mathbf{M} + 7\mathbf{S}$. We also provide methods for recovering the missing $X$-coordinate. Compared to earlier work like [6], [9] or the formulas on EFD, we explicitly consider all formulas also for the case $c \neq 1$, even though one would typically use in applications curves with $c = 1$.

The second parametrization also omits the $X$-coordinate. Additionally it uses the squares of the coordinates of the points only. On elliptic curves in generalized Edwards form, addition can be done with $5\mathbf{M}+2\mathbf{S}$ and point doubling with $5\mathbf{S}$. We also provide a tripling formula for this second representation. For point doubling we get completely rid of multiplications and employ squarings in the ground field only. This is desirable since squarings can be done slightly faster than generic multiplications, see for example [7]. This second representation is best suited when employed in a scalar multiplication. Again we explicitly consider all formulas also for the case $c \neq 1$. On EFD several formulas for this parametrization can be found, but only for the special case $c = 1$ and $d$ being a square in the ground field. The idea of this representation can already be found in Gaudry and Lubicz [9], section 6.2.

The plan of the paper is as follows. We recall the basics of Edwards coordinates in the next section and describe the addition, doubling and tripling formula in section 3. The formula for recovering the $X$-coordinate is given in section 4. The parametrization of the points that uses the squares of the coordinates only is analyzed in section 5.

## 2 Edwards Form

We describe now the basics of elliptic curves in generalized Edwards form. More details can be found for example in [3, 4]. Such curves are given by equations of the form

$$E_{c,d}: x^2 + y^2 = c^2(1 + dx^2y^2),$$

where $c, d$ are curve parameters in a field $k$ of characteristic different from 2. When $c, d \neq 0$ and $dc^4 \neq 1$, the addition law is defined by

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

For this addition law, the point $(0, c)$ is the neutral element. The inverse of a point $P = (x, y)$ is $-P = (-x, y)$. In particular, $(0, -c)$ has order 2; $(c, 0)$ and $(-c, 0)$ are the points of order 4. When the curve parameter $d$ is not a square in $k$, then the addition law (1) is complete (i.e. defined for all inputs).

## 3 Representing Points in Edwards Form

As explained in the introduction, we represent a point $P$ on the curve $E_{c,d}$ using projective coordinates $P = (Y_1 : Z_1)$. Write $[n]P = (Y_n : Z_n)$. Then we have

**Theorem 1.** *Let $E_{c,d}$ be an elliptic curve in generalized Edwards form defined over a field $k$, such that* $\mathrm{char}(k) \neq 2$ *and $c, d \neq 0$, $dc^4 \neq 1$ and $d$ is not a square in $k$. Then for $m > n$ we have*

$$\begin{aligned} Y_{m+n} &= Z_{m-n}\left(Y_m^2(Z_n^2 - c^2dY_n^2) + Z_m^2(Y_n^2 - c^2Z_n^2)\right), \\ Z_{m+n} &= Y_{m-n}\left(dY_m^2(Y_n^2 - c^2Z_n^2) + Z_m^2(Z_n^2 - c^2dY_n^2)\right). \end{aligned}$$

*It can be computed using* $6\mathbf{M} + 4\mathbf{S}$. *When* $n = m$, *the doubling formula is given by*

$$Y_{2n} = -c^2 d Y_n^4 + 2Y_n^2 Z_n^2 - c^2 Z_n^4,$$
$$Z_{2n} = d Y_n^4 - 2c^2 d Y_n^2 Z_n^2 + Z_n^4,$$

*which can be computed using* $1\mathbf{M} + 4\mathbf{S}$.

On EFD one finds related formulas for $c = 1$ and $d$ being a square in $k$. We defer a detailed study of the relationship between the formulas given there and ours to the end of this section.

*Proof.* Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two different points on the curve $E_{c,d}$. Since the curve parameter $d$ is not a square in $k$, the addition law (1) is defined for all inputs. Let $P_1 + P_2 = (x_3, y_3)$ and $P_1 - P_2 = (x_4, y_4)$. Then the addition law (1) gives

$$y_3 c(1 - d x_1 x_2 y_1 y_2) = y_1 y_2 - x_1 x_2,$$
$$y_4 c(1 + d x_1 x_2 y_1 y_2) = y_1 y_2 + x_1 x_2.$$

After multiplying the two equations above, we obtain

$$y_3 y_4 c^2 (1 - d^2 x_1^2 x_2^2 y_1^2 y_2^2) = y_1^2 y_2^2 - x_1^2 x_2^2. \tag{2}$$

Next we substitute $x_1^2 = \frac{c^2 - y_1^2}{1 - c^2 d y_1^2}$ and $x_2^2 = \frac{c^2 - y_2^2}{1 - c^2 d y_2^2}$ (obtained from the curve equation) in (2) yielding

$$y_3 y_4 (-d y_1^2 y_2^2 + c^2 d y_1^2 + c^2 d y_2^2 - 1) = c^2 d y_1^2 y_2^2 - y_1^2 - y_2^2 + c^2. \tag{3}$$

After switching to projective coordinates, we see that for $m > n$ the formula for adding $[m]P = (Y_m, Z_m)$ and $[n]P = (Y_n, Z_n)$ becomes

$$\frac{Y_{m+n}}{Z_{m+n}} \frac{Y_{m-n}}{Z_{m-n}} = \frac{Y_m^2 (Z_n^2 - c^2 d Y_n^2) + Z_m^2 (Y_n^2 - c^2 Z_n^2)}{d Y_m^2 (Y_n^2 - c^2 Z_n^2) + Z_m^2 (Z_n^2 - c^2 d Y_n^2)}. \tag{4}$$

This proves the addition formula. If $P_1 = P_2$, we obtain by the addition law (1)

$$y_3 c(1 - d x_1^2 y_1^2) = y_1^2 - x_1^2.$$

Similarly, if we substitute $x_1^2 = \frac{c^2 - y_1^2}{1 - c^2 d y_1^2}$ into the equation above to obtain

$$y_3 (c d y_1^4 - 2c^3 d y_1^2 + c) = -c^2 d y_1^4 + 2y_1^2 - c^2.$$

This proves the doubling formula in Theorem 1 after switching to projective coordinates. □

We obtain additional savings in the case $c = 1$:

**Corollary 1.** *Assume the same as in Theorem 1. If $c = 1$ we have for $m > n$*

$$Y_{m+n} = Z_{m-n}\left((Y_m^2 - Z_m^2)(Z_n^2 - dY_n^2) - (d-1)Y_n^2 Z_m^2\right),$$
$$Z_{m+n} = -Y_{m-n}\left((Y_m^2 - Z_m^2)(Z_n^2 - dY_n^2) + (d-1)Y_m^2 Z_n^2\right),$$

*which can be computed using $5\mathbf{M} + 4\mathbf{S}$. For doubling we obtain*

$$Y_{2n} = -(Y_n^2 - Z_n^2)^2 - (d-1)Y_n^4,$$
$$Z_{2n} = (dY_n^2 - Z_n^2)^2 - d(d-1)Y_n^4,$$

*which can be computed using $5\mathbf{S}$.* □

*Remark 1.* A simple induction argument shows that the computation of the $2^j$-fold of a point can be computed using $5j\mathbf{S}$.

A slight variant of the doubling formula in this Corollary is given by Castryck, Galbraith and Farashahi [6] in their section 3. On EFD similar doubling formulas can be found, but only for the special case of $d$ being a square in the ground field. For general $c$ the formulas of Theorem 1 do not seem to be in the literature.

In the remainder of this section we will explore this relationship in more detail. We focus here in particular on Corollary 1 since EFD covers the case $c = 1$ only. As on EFD we assume now that $d = r^2$ for some $r \in k$. Then we can write

$$y_{2n} = \frac{-r^2 Y_{2n}^4 + 2Y_{2n}^2 Z_{2n}^2 - Z_{2n}^4}{r^2 Y_{2n}^4 - 2r^2 Y_{2n}^2 Z_{2n}^2 + Z_{2n}^4},$$

where $y_{2n}$ denotes the corresponding affine $y$-coordinate of the point. Thus we have

$$ry_{2n} = \frac{2r/(r-1) \cdot \left(r^2 Y_{2n}^4 - 2Y_{2n}^2 Z_{2n}^2 + Z_{2n}^4\right)}{-2/(r-1) \cdot (r^2 Y_{2n}^4 - 2r^2 Y_{2n}^2 Z_{2n}^2 + Z_{2n}^4)}.$$

If we set $A := \frac{1+r}{1-r}(rY_{2n}^2 - Z_{2n}^2)^2$ and $B := (rY_{2n}^2 + Z_{2n}^2)^2$ we can write the numerator of the last expression as $B - A$ and the denominator as $B + A$, yielding the formulas `dbl-2006-g` and `dbl-2006-g-2` from EFD. This can be computed with $4\mathbf{S}$, but only for those restricted curve parameters.

The addition formulas `dadd-2006-g` and `dadd-2006-g-2` from EFD can be deduced in a similar way from our differential addition formula in Corollary 1.

### 3.1 A Tripling Formula

One also obtains a tripling formula that can be computed using $4\mathbf{M}+7\mathbf{S}$. This is cheaper than by doing first a doubling and afterwards an addition, which costs $7\mathbf{M} + 8\mathbf{S}$ ($5\mathbf{M} + 9\mathbf{S}$ when $c = 1$).

**Proposition 1.** *Assume the same as in Theorem 1. Furthermore let* $\mathrm{char}(k) \neq 3$. *Then we have*

$$Y_{3n} = Y_n(c^2(3Z_n^4 - dY_n^4)^2 - Z_n^4(8c^2Z_n^4 + (Y_n^2(c^3d + c^{-1}) - 2cZ_n^2)^2 - c^{-2}(c^4d + 1)^2Y_n^4)),$$
$$Z_{3n} = Z_n(c^2(Z_n^4 - 3dY_n^4)^2 + dY_n^4(4c^2Z_n^4 - (Y_n^2(c^3d + c^{-1}) - 2cZ_n^2)^2 + c^{-2}((c^4d + 1)^2 - 12c^4d)Y_n^4)),$$

*which can be computed using* $4\mathbf{M} + 7\mathbf{S}$.

*Proof.* Let $(x_3, y_3) = 3(x, y) = 2(x, y) + (x, y)$. Using the addition law (1), we obtain an expression for $y_3$. Inside the expression, make the substitution $x^2 = \frac{c^2 - y^2}{1 - c^2dy^2}$ and simplify to obtain an expression in $y$ only. Then we have

$$y_3 = \frac{y(c^2d^2y^8 - 6c^2dy^4 + 4(c^4d + 1)y^2 - 3c^2)}{-3c^2d^2y^8 + 4d(c^4d + 1)y^6 - 6c^2dy^4 + c^2}.$$

Switch to projective coordinates $y = Y/Z$ and rearrange terms. The formula follows. □

**Corollary 2.** *Assume the same as in Theorem 1. Furthermore let* $\mathrm{char}(k) \neq 3$ *and assume* $c = 1$. *Then we have*

$$Y_{3n} = Y_n((dY_n^4 - 3Z_n^4)^2 - Z_n^4((2Z_n^2 - (1 + d)Y_n^2)^2 + 8Z_n^4 - (1 + d)^2Y_n^4)),$$
$$Z_{3n} = Z_n((Z_n^4 - 3dY_n^4)^2 - dY_n^4((2Z_n^2 - (1 + d)Y_n^2)^2 - 4Z_n^4 + (12d - (1 + d)^2)Y_n^4)),$$

*which can be computed using* $4\mathbf{M} + 7\mathbf{S}$. □

## 4 Recovering the $x$-coordinate

In some cryptographic applications it is important to have at some point both: $x$- *and* $y$-coordinates. Theorem 2 shows how to obtain them. There have been results [13, 5] in this direction for other forms of elliptic curves. To recover the (affine) $x$-coordinate, we need the following

**Proposition 2.** *Fix an elliptic curve* $E_{c,d}$ *in generalized Edwards form such that* $\mathrm{char}(k) \neq 2$ *and* $c, d \neq 0$, $dc^4 \neq 1$ *and* $d$ *is not a square in* $k$. *Let* $Q = (x, y)$, $P_1 = (x_1, y_1)$ *be two points on* $E_{c,d}$. *Define* $P_2 = (x_2, y_2)$ *and* $P_3 = (x_3, y_3)$ *by* $P_2 = P_1 + Q$ *and* $P_3 = P_1 - Q$. *Then we have*

$$x_1 = \frac{2yy_1 - cy_2 - cy_3}{cdxyy_1(y_3 - y_2)}, \tag{5}$$

*provided the denominator does not vanish.*

*Proof.* By the addition law (1), we have

$$c(1 - dxx_1yy_1)y_2 = yy_1 - xx_1,$$
$$c(1 + dxx_1yy_1)y_3 = yy_1 + xx_1.$$

Add the two equations and solve for $x_1$, and the Proposition follows. □

The following lemma provides a simple criterion, which tells us when the denominator in formula (5) does not vanish.

**Lemma 1.** *Assume the same as in Proposition 2. Furthermore, let $P_1, Q$ be points whose order does not divide 4. Then the formula (5) holds.*

*Proof.* The points $P_1$ and $Q$ have orders that are not $1, 2, 4$, so $x, x_1, y, y_1 \neq 0$. Suppose now $y_2 = y_3$ (i.e. $y$-coordinates of $P_1 + Q$ and $P_1 - Q$ are the same). By the addition law (1), this implies

$$\frac{yy_1 - xx_1}{c(1 - dxx_1yy_1)} = \frac{yy_1 + xx_1}{c(1 + dxx_1yy_1)}.$$

By solving for $d$ it follows that $dy^2y_1^2 = 1$, which is a contradiction since $d$ is not a square in $k$.

We are now ready to prove

**Theorem 2.** *Let $E_{c,d}$ be an elliptic curve in generalized Edwards form defined over a field $k$ such that $\mathrm{char}(k) \neq 2$, $c, d \neq 0$, $dc^4 \neq 1$ and $d$ is not a square in $k$. Let $P = (x, y)$ be a point whose order does not divide 4. Let $y_n, y_{n+1}$ be the affine $y$-coordinates of the points $[n]P, [n+1]P$ respectively. Then we have*

$$x_n = \frac{2yy_ny_{n+1} - cC_n - cy_{n+1}^2}{cdxyy_n\left(C_n - y_{n+1}^2\right)},$$

*where*

$$A = 1 - c^2dy^2,$$
$$B = y^2 - c^2,$$
$$C_n = \frac{Ay_n^2 + B}{dBy_n^2 + A}.$$

*Proof.* Let $[n]P = (x_n, y_n)$, where $P$ is not a 4-torsion point on $E_{c,d}$. Our task is to recover $x_n$. By Proposition 2 with $P_1 = [n]P$ and $Q = (x, y)$, we may write

$$x_n = \frac{2yy_n - cy_{n-1} - cy_{n+1}}{cdxyy_n(y_{n-1} - y_{n+1})}, \tag{6}$$

where $y_{n-1}$,$y_{n+1}$ are the $y$-coordinates of the points $[n-1]P$ and $[n+1]P$ respectively. Now the variable $y_{n-1}$ can be eliminated because of (4). Indeed we may write using (4) in affine coordinates

$$y_{n-1}y_{n+1} = \frac{Ay_n^2 + B}{dBy_n^2 + A}, \tag{7}$$

where

$$A = 1 - c^2dy^2, \quad B = y^2 - c^2.$$

Now from (7), $y_{n-1}$ can be isolated and put back in (6). This gives

$$x_n = \frac{2yy_ny_{n+1}(dBy_n^2 + A) - c(Ay_n^2 + B) - cy_{n+1}^2(dBy_n^2 + A)}{cdxyy_n\left(Ay_n^2 + B - y_{n+1}^2(dBy_n^2 + A)\right)}.$$

The claim follows. □

## 5 A parametrization using squares only

The formulas in Theorem 1 show that for the computation of $Y_{m+n}^2$ and $Z_{m+n}^2$ it is sufficient to know the squares of the coordinates of the points $(Y_m : Z_m)$, $(Y_n : Z_n)$ and $(Y_{m-n} : Z_{n-m})$ only. This gives

**Theorem 3.** *Assume the same as in Theorem 1. Then for $m > n$ we have*

$$\begin{aligned} Y_{m+n}^2 &= Z_{m-n}^2\left((A+B)/2\right)^2, \\ Z_{m+n}^2 &= Y_{m-n}^2\left((A-B)/2 + (d-1)Y_m^2(Y_n^2 - c^2Z_n^2)\right)^2, \end{aligned}$$

*with*

$$\begin{aligned} A &:= (Y_m^2 + Z_m^2)((1-dc^2)Y_n^2 + (1-c^2)Z_n^2), \\ B &:= (Y_m^2 - Z_m^2)((1+c^2)Z_n^2 - (1+dc^2)Y_n^2). \end{aligned}$$

*This addition can be computed using $5\mathbf{M} + 2\mathbf{S}$ if one stores the squares of the coordinates only. When $n = m$, we obtain*

$$\begin{aligned} Y_{2n}^2 &= \left((1-c^2d)Y_n^4 + (1-c^2)Z_n^4 - (Y_n^2 - Z_n^2)^2\right)^2, \\ Z_{2n}^2 &= \left(dc^2(Y_n^2 - Z_n^2)^2 - d(c^2-1)Y_n^4 + (c^2d-1)Z_n^4\right)^2, \end{aligned}$$

*which can be computed using $5\mathbf{S}$ if one stores the squares of the coordinates only.*

*Proof.* This follows directly from Theorem 1 and elementary calculus. □

A direct adaption of Corollary 1 does not give any speedup. Again on EFD one finds related formulas for $c = 1$ and $d$ being a square in $k$.

We will now sketch the computation of a scalar multiple $[s]P$ in this parametrization. Assume $P$ has affine coordinates $(x : y)$. Then one would proceed as follows: After changing to projective coordinates $(X : Y : Z)$, two squares (one for each of the coordinates $Y$ and $Z$) have to be computed. Now a differential addition chain is employed to compute the multiple $[s]P$. During all but the last step of the computation we store the squares of the coordinates of the intermediate points only. The last step plays a special role now, since we wish to obtain at the end the coordinates of the point $[s]P$ and not the square of the coordinates. To do so, we run the last step using the first parametrization. If we construct from the beginning the differential addition chain such that for each computation of $P_{m+n}$ we have that $m - n = 1$, we obtain an efficient algorithm for computing the scalar multiple $[s]P$ on an elliptic curve in generalized Edwards form using the second parametrization. In order to recover then the $x$-coordinate one would have to compute also the scalar multiple $[s+1]P$ and use the recovering formula from Theorem 2.

Also the tripling formula given in Proposition 1 can be adapted to this second parametrization. Namely we have

**Corollary 3.** *Assume the same as in Theorem 1. Furthermore, we assume* $\mathrm{char}(k) \neq 3$. *Then we have*

$$\begin{aligned} Y_{3n}^2 = Y_n^2(c^2(3Z_n^4 - dY_n^4)^2 - Z_n^4(8c^2Z_n^4 + (Y_n^2(c^3d + c^{-1}) - 2cZ_n^2)^2 \\ - c^{-2}(c^4d + 1)^2Y_n^4))^2, \\ Z_{3n}^2 = Z_n^2(c^2(Z_n^4 - 3dY_n^4)^2 + dY_n^4(4c^2Z_n^4 - (Y_n^2(c^3d + c^{-1}) - 2cZ_n^2)^2 \\ + c^{-2}((c^4d + 1)^2 - 12c^4d)Y_n^4))^2, \end{aligned}$$

*which can be computed using* $4\mathbf{M}+7\mathbf{S}$ *if one stores the squares of the coordinates only.* □

## 6 Acknowledgments

This work was funded by the B-IT foundation and the state of North Rhine-Westphalia.

## References


1. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted edwards curves. In S. Vaudenay, editor, *Progress in Cryptology: Proceedings of AFRICACRYPT 2008,* Casablanca, Morocco, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405, 2008.
2. D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. ECM using edwards curves. 2008.
3. D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *Advances in Cryptology: Proceedings of ASIACRYPT 2007,* Kuching, Sarawak, Malaysia, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50, June 2007.
4. D. J. Bernstein and T. Lange. Inverted edwards coordinates. In S. Boztas and H. feng Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings*, volume 4851 of *Lecture Notes in Computer Science*, pages 20–27, 2007.
5. É. Brier and M. Joye. Weierstraß elliptic curves and side-channel attacks. In D. Naccache and P. Paillier, editors, *Public Key Cryptography*, number 2274 in Lecture Notes in Computer Science, pages 183–194, Berlin, Heidelberg, 2002. Springer-Verlag.
6. W. Castryck, S. Galbraith, and R. R. Farashahi. Efficient arithmetic on elliptic curves using a mixed edwards-montgomery representation. Cryptology ePrint Archive, Report 2008/218, 2008.
7. H. Cohen and G. Frey. *Handbook of Elliptic and Hyperelliptic Curve Cryptography; written with Roberto M. Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen and Frederik Vercauteren.* Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2006.
8. H. M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3):393–422, July 2007.
9. P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 kummer surfaces and of elliptic kummer lines. *Finite Fields and Their Applications*, 15(2):246 – 260, 2009.
10. Information Technology Laboratory. Fips 186-3: Digital signature standard (dss). Technical report, National Institute of Standards and Technology, June 2009.
11. H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.
12. P. L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, January 1987.
13. K. Okeya and K. Sakurai. Efficient elliptic curve cryptosystem from a scalar multiplication algorithm with recovery of the y-coordinate on a montgomery-form elliptic curve. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems, Workshop, CHES'01,* Paris, France, number 2162 in Lecture Notes in Computer Science, pages 126–141, Berlin, Heidelberg, 2001. Springer-Verlag.