# Differential Addition in Edwards Coordinates Revisited and a Short Note on Doubling in Twisted Edwards Form

Srinivasa Rao Subramanya Rao
*Mathematical Sciences Institute, The Australian National University, Union Lane, Canberra ACT 2601, Australia*

Keywords: Scalar Multiplication, Montgomery Curves, Differential Addition, Edwards Curves, Twisted Edwards Curves, Binary Edwards Curves, Homogeneous Projective, Inverted Coordinates, Extended Homogeneous Projective Coordinates, w-coordinate Differential addition.

Abstract: Cryptographic algorithms in smart cards and other constrained environments increasingly rely on Elliptic Curves and thus it is desirable to have fast algorithms for elliptic curve arithmetic. In this paper, we provide

(i) faster differential addition formulae for elliptic curve arithmetic on Generalized Edwards' Curves improving upon the currently known formulae in the literature, proposed by Justus and Loebenberger at IWSEC 2010,

(ii) more efficient affine differential addition formulae for a new model of Binary Edwards Curves proposed by Wu, Tang and Feng at INDOCRYPT 2012 and

(iii) an algorithm for point doubling on Twisted Edwards Curves with a smaller footprint when the implementation is desired to work across Homogeneous Projective, Inverted and Extended Homogeneous Projective Coordinates.

## 1 INTRODUCTION

Security in smart devices and mobile networks require an efficient implementation of cryptographic algorithms owing to the computational, bandwidth, power and memory constraints experienced in these environments. With its smaller key sizes, Elliptic Curve Cryptography(ECC) is increasingly seen as an alternative to traditional public key algorithms such as RSA, especially in constrained environments such as mobile devices. Thus while ECC is attractive for the success of lightweight applications such as security for mobile and/or embedded applications, RFID and in the context of "Internet for Things", optimized low-cost ECC implementations are crucial for this success.

In recent years, amongst other things, research in ECC has focused on efficient implementations. As is well known, the set of points on an elliptic curve defined over a finite field along with the point at infinity form a group when appropriate group operations are defined. Elliptic curve groups have an additive notation and thus the operation of exponentiation in a group with multiplicative notation becomes a multiplication operation in Elliptic curve groups over a finite field. Point multiplication is at the core of most ECC applications and dominates ECC. Thus efficient methods for point multiplication are crucial for ECC. A very good source for point multiplication formula is the EFD(Explicit Forms Database) (Bernstein and Lange, 2007). The usual convention in the literature is to denote the cost of a field inversion by $I$, a field multiplication by $M$ and a field squaring by $S$. In this paper we will denote the cost of a field multiplication with a constant by $M_c$. Field Multiplications by $2, 3$ or $4$ can be achieved by field additions and are thus ignored in cost comparisons in this paper. Lately, a new form of an elliptic curve called "Edwards Curve" has received attention in the research community mainly due to its low finite field operation count for point multiplication. Differential addition, a concept used earlier in the context of Montgomery curves has been adapted to other forms of elliptic curves including Edwards curves.

In this paper, we review some formulae presented in the literature towards differential addition on Edwards Curves and work towards speeding up the same. Specifically, we look at formulae proposed by Justus and Loebenberger at IWSEC 2010 and at formulae proposed by Wu, Tang and Feng at INDOCRYPT 2012. The rest of the paper is organized as follows: In Section-2, we review (i) differential addition and (ii) some formulae



Rao, S.
Differential Addition in Edwards Coordinates Revisited and a Short Note on Doubling in Twisted Edwards Form.
DOI: 10.5220/0005970603360343
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT*, pages 336-343
ISBN: 978-989-758-196-0

presented in the literature for differential addition on Generalized Edwards Curves and Binary Edwards Curves. In section 3, we provide faster algorithms to evaluate some of the formulae reviewed in Section 2. In Section 4, we review point doubling in Twisted Edwards Curves for the Homogeneous Projective, Inverted and Extended Homogeneous Projective coordinate forms and provide an alternate algorithm for point doubling. This alternate algorithm does not improve on the operation counts of currently known algorithms in the literature, but the similarity of the algorithms across coorodinate forms means that it may be possible to have a smaller footprint when implementing algorithms that work with all of these three coordinate systems simultaneously. We finally conclude in Section-4.

## 2 DIFFERENTIAL ADDITION

The problem of reducing the number of group operations required while computing an exponentiation (multiplication whilst in a additive group) is probably best seen in the context of addition chains. A finite sequence of integers $a_0, a_1, \ldots a_r$ is called an addition chain (section 4.63 in (D.Knuth, 1998)) for $a_r$ if for each element $a_i$, there exists $a_j$ and $a_k$ in the sequence such that $a_0 = 1$ and for all $i = 1, 2, \ldots, r$

$$a_i = a_j + a_k, \quad \text{for some } k \leq j < i \tag{1}$$

Addition chains are applicable both in the context of multiplicative groups and additive groups such as Elliptic curve groups over a finite field.

In 1987, Montgomery proposed a special type of an elliptic curve, now known as Montgomery form of an elliptic curve or simply Montgomery curve (P.L.Montgomery, 1987). The arithmetic on a Montgomery curve relies on '$x$-coordinate' only arithmetic and also requires the 'difference' of two group elements (points) to be known prior to the computation of addition of these two elements. Thus ordinary addition chains and improvements of these chains cannot be directly utilized for scalar multiplication on Montgomery curves where '$x$-coordinate' only formale are used. A special form of addition chain called Lucas chains is useful in this context. A Lucas chain is a restricted variant of an addition chain where the indices in equation (1) above are such that either $j = k$ or the difference $a_k - a_j$ is already part of the chain. A special case of Lucas chains occur when either $j = k$ or $a_k - a_j = a_0 = 1$ and these are called binary chains. A good reference for Lucas chains is (Montgomery, 1992). Lucas chains are also known as differential addition chains in the literature (Bernstein, 2006b). Below we review differential addition formulae for Montgomery curves. A Montgomery curve defined over a finite field $F_p$ is given by

$$E_m : By^2 = x^3 + Ax^2 + x$$

If $P = (x_1, y_1)$ is a point on the $E_m$, $P$ can be written in projective coordinates as $P = (X_1, Y_1, Z_1)$. If $[n]P = (X_n : Y_n : Z_n)$, the sum $[n+m]P = [n]P + [m]P$ can be computed using the differential addition formulae below:

**Addition:** $(n \neq m)$

$$X_{m+n} = Z_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$
$$Z_{m+n} = X_{m-n}((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n))^2$$

**Doubling:** $(n = m)$

$$4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2$$
$$Z_{2n} = 4X_nZ_n((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n))$$

In the above formulae, we can see that the $Y$-coordinate is not required in the computation of $X$-coordinate of $[n+m]P$, provided we are supplied with the value of $[n-m]P$. This is employed by the Montgomery ladder for scalar multiplication. A good reference for Montgomery ladders is (M.Joye and S.Yen, 2002).

The idea of differential addition has been extended to other forms of elliptic curves. Lopez and Dahab (J.Lopez and R.Dahab, 1999) generalized this idea to Weierstrass form binary curves and Brier and Joye (E.Brier and M.Joye, 2002) generalized it to Weierstrass Curves defined over $GF(p)$. Justus and Loebenberger (R.Justus and Loebenberger, 2010) extended differential addition to Generalized Edwards Elliptic Curve form in a paper presented at IWSEC 2010. Wu, Tang and Feng (H.Wu et al., 2012) proposed differential addition formulae for a new model of Binary elliptic curves. In this paper, we try to speed up some of the formulae proposed in (R.Justus and Loebenberger, 2010) and the affine $w$-Coordinate differential addition proposed in (H.Wu et al., 2012). In the remainder of this section, we review some of the Differential addition formulae for Generalized Edwards' Curves as provided in (R.Justus and Loebenberger, 2010) and the affine $w$-Coordinate differential addition formulae for a new model of Binary elliptic curve as provided in (H.Wu

et al., 2012).

Generalized Edwards Curves over a finite field $F_p$ are given by (curve parameters $c,d \in F_p$)

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

It turns out that the differential addition formulae for generalized Edwards curves uses $y$-only coordinates instead of $x$-only coordinates for Montgomery curves. Let $P = (x_1, y_1)$ be a point on $E_{c,d}$. In projective coordinates, $P$ can be written as $P = (X_1, Y_1, Z_1)$ and let $[n]P = (X_n : Y_n : Z_n)$. If $c,d \neq 0$, $dc^4 \neq 1$ and $d$ is not a square in $GF(p)$, the sum $[n+m]P = [n]P + [m]P$, as provided in (R.Justus and Loebenberger, 2010) is reproduced below:

**A. Differential Addition for Generalised Edwards Coordinates:** $m > n$

(Operation count given by authors in (R.Justus and Loebenberger, 2010) is $6M + 4S$).

$$Y_{m+n} = Z_{m-n}(Y_m^2(Z_n^2 - c^2dY_n^2) + Z_m^2(Y_n^2 - c^2Z_n^2))$$
$$Z_{m+n} = Y_{m-n}(dY_m^2(Y_n^2 - c^2Z_n^2) + Z_m^2(Z_n^2 - c^2dY_n^2))$$

**B. Differential Doubling for Generalised Edwards Coordinates:** $n = m$

(Operation count given by authors in (R.Justus and Loebenberger, 2010) is $1M + 4S$).

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

In (R.Justus and Loebenberger, 2010), point tripling formula are provided as well, which we reproduce below:

**C. Tripling for Generalised Edwards Coordinates:**

(Operation count given by authors in (R.Justus and Loebenberger, 2010) is $4M + 7S$).

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

In (R.Justus and Loebenberger, 2010), an alternate parameterization is provided by the authors, where only the squares of the points $(Y_m : Z_m)$, $(Y_n : Z_n)$ and $(Y_{m-n} : Z_{m-n})$ are utilized. We call this "Squares Only" or SQO parametrization. The authors provide addition, doubling and tripling formulae for this parametrization. Here we reproduce the doubling and the tripling formulae from (R.Justus and Loebenberger, 2010) for SQO parametrization.

**D. SQO Doubling for Generalised Edwards Coordinates:** $n = m$

(Operation count given in (R.Justus and Loebenberger, 2010) is $5S$).

$$Y_{2n}^2 = ((1 - c^2d)Y_n^4 + (1 - c^2)Z_n^4 - (Y_n^2 - Z_n^2)^2)^2$$
$$Z_{2n}^2 = (dc^2(Y_n^2 - Z_n^2)^2 - d(c^2 - 1)Y_n^4 + (c^2d - 1)Z_n^4)^2$$

**E. SQO Tripling for Generalised Edwards Coordinates:** $m = 2n$

(Operation count in (R.Justus and Loebenberger, 2010) is $4M + 7S$).

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

In (H.Wu et al., 2012), the authors propose a new model of Binary Edwards Curve given by

$$S_t : x^2y + xy^2 + txy + x + y = 0$$

where $(x,y) \in K^2$ and $K$ is a field of characteristic 2. Further, in section 6 of this paper, the authors construct differential addition formula for $S_t$. We reproduce the approach and the formulae here.

**F. Affine $w$-coordinate Differential Addition and Doubling for a new model of Binary Edwards Curves proposed in (H.Wu et al., 2012):**

(Operation count for addition and doubling as given in (H.Wu et al., 2012) is $1I + 2M + 2S + 1M_c$ and $1I + 1M + 2S + 1M_c$ respectively.)

Utilizing $w$-coordinate differential addition that was initially proposed by Bernstein in (Bernstein et al., 2008a), the authors in (H.Wu et al., 2012) propose $w$-coordinate differential addition and doubling for $S_t$, i.e., they present formulae to compute $w(P+Q)$ and $w(2P)$ from $w(P)$, $w(Q)$ and $w(Q-P)$. If $P = (x,y)$ is a point on $S_t$, then the $w$-function is defined as $w(P) = xy$. If $P = (x_2,y_2)$, $Q = (x_3,y_3)$, $Q - P = (x_1,y_1)$, $2P = (x_4,y_4)$ and $Q + P = (x_5,y_5)$, we write $w_i = x_iy_i$ for $i = 1,2,3,4,5$. Then $w_2 = w(P)$, $w_4 = w(2P)$, $w_5 = w(P+Q)$, $w_1 = w(Q-P)$ and $w_3 = w(Q)$. The affine differential addition formulae on $S_t$, as developed and presented in (H.Wu et al., 2012) are as follows:

$$w_4 = \frac{1 + w_2^4}{t^2w_2^2} \text{ and } w_5 = w_1 + \frac{t^2w_2w_3}{w_2^2 + w_3^2}$$

# 3 ALTERNATE ALGORITHMS AND NEWER OPERATION COUNTS

In this section we show that the operation counts in formulae (B-F) of Section 2 can be improved. For clarity in comparison, the subsections that describe and compare our improvements to (B-F) of Section-2 are labeled as (BB-FF) respectively.

**BB. Differential Doubling for Generalised Edwards Coordinates:**
The operation count of formula (B) in Section 2 is $1M + 4S$ as the formula can be computed using the following algorithm:

| | | |
|---|---|---|
| $A \leftarrow Y_n^2$ | $(=Y_n^2)$ | $S$ |
| $B \leftarrow Z_n^2$ | $(=Z_n^2)$ | $S$ |
| $D \leftarrow A * B$ | $(=Y_n^2 Z_n^2)$ | $M$ |
| $A \leftarrow A^2$ | $(=Y_n^4)$ | $S$ |
| $B \leftarrow B^2$ | $(=Z_n^4)$ | $S$ |
| $Y_{2n} = -c^2 dA +$ $2D - c^2 B$ | $(= -c^2 dY_n^4 +$ $2Y_n^2 Z_n^2 - c^2 Z_n^4)$ | $2M_c$ |
| $Z_{2n} = dA - 2c^2 dD + B$ | $(= dY_n^4 -$ $2c^2 dY_n^2 Z_n^2 + Z_n^4)$ | $2M_c$ |

Thus the total complexity, if one takes into consideration the cost of multiplication by a constant other than 1 or 2 or 3, is $(1M + 4M_c + 4S)$. The formulae (B) in Section 2 can be rewritten as

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

The rewritten formulae above can be computed using the algorithm below:

| | | |
|---|---|---|
| $A \leftarrow Y_n^2$ | $(=Y_n^2)$ | $S$ |
| $B \leftarrow Z_n^2$ | $(=Z_n^2)$ | $S$ |
| $E \leftarrow A^2$ | $(=Y_n^4)$ | $S$ |
| $F \leftarrow B^2$ | $(=Z_n^4)$ | $S$ |
| $G \leftarrow (A+B)^2$ $-E-F$ | $(=2Y_n^2 Z_n^2)$ | $S$ |
| $Y_{2n} = G -$ $c^2(F+dE)$ | $(=2Y_n^2 Z_n^2 -$ $c^2(Z_n^4 + dY_n^4))$ | $2M_c$ |
| $Z_{2n} = (-c^2 d)G +$ $(F+dE)$ | $(=-c^2 d(2Y_n^2 Z_n^2) +$ $(Z_n^4 + dY_n^4))$ | $1M_c$ |

Thus the new complexity is $5S + 3M_c$. As $1S < 1M$, the new complexity $5S + 3M_c$ is less than the older complexity $(1M + 4M_c + 4S)$

**CC. Tripling for Generalised Edwards Coordinates:**
The operation count of formula (C) in Section 2 of this paper is $4M + 7S$. In addition to this, by inspection, one can count $8M_c$ operations as required to compute the requisite formula. Thus the total complexity of formula(C) is $4M + 7S + 8M_c$
From section 3.1 in (R.Justus and Loebenberger, 2010), we have

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

writing $y = Y/Z$ in projective coordinates, the above formula can be written as

$$\frac{Y_{3n}}{Z_{3n}} = \frac{Y_n}{Z_n} \cdot \frac{(c^2 d^2 Y_n^8 - 6c^2 dY_n^4 Z_n^4 + 4(c^4 d + 1)Y_n^2 Z_n^6 - 3c^2 Z_n^8)}{-3c^2 d^2 Y_n^8 + 4d(c^4 d + 1)Y_n^6 Z_n^2 - 6c^2 dY_n^4 Z_n^4 + c^2 Z_n^8}$$

Then

$$Y_{3n} = Y_n[c^2 d^2 Y_n^8 - 6c^2 dY_n^4 Z_n^4 + 4(c^4 d + 1)Y_n^2 Z_n^6 - 3c^2 Z_n^8]$$

and

$$Z_{3n} = Z_n[-3c^2 d^2 Y_n^8 + 4d(c^4 d + 1)Y_n^6 Z_n^2 - 6c^2 dY_n^4 Z_n^4 + c^2 Z_n^8]$$

The above rewritten formulae can now be computed using the algorithm below:

| | | |
|---|---|---|
| $A \leftarrow Y_n^2$ | $(=Y_n^2)$ | $S$ |
| $B \leftarrow Z_n^2$ | $(=Z_n^2)$ | $S$ |
| $E \leftarrow A^2$ | $(=Y_n^4)$ | $S$ |
| $F \leftarrow B^2$ | $(=Z_n^4)$ | $S$ |
| $G \leftarrow (A+B)^2$ $-E-F$ | $(=(Y_n^2 + Z_n^2)^2$ $-Y_n^4 - Z_n^4 = 2Y_n^2 Z_n^2)$ | $S$ |
| $H \leftarrow G^2$ | $(=4Y_n^4 Z_n^4)$ | $S$ |
| $J \leftarrow E^2$ | $(=Y_n^8)$ | $S$ |
| $K \leftarrow F^2$ | $(=Z_n^8)$ | $S$ |
| $M \leftarrow (G+F)^2$ $-K-H$ | $[=(2Y_n^2 Z_n^2 + Z_n^4)^2 - Z_n^8$ $-4Y_n^4 Z_n^4] = 4Y_n^2 Z_n^6$ | $S$ |
| $N \leftarrow (G+E)^2$ $-J-H$ | $[=(2Y_n^2 Z_n^2 + Y_n^4)^2$ $-Y_n^8 - 4Y_n^4 Z_n^4] = 4Y_n^6 Z_n^2$ | $S$ |

Finally,
$Y_{3n} \leftarrow Y_n[(c^2 d^2)J - (\frac{3}{2}c^2 d)H + (c^2 d + 1)M - (3c^2)K]$
which costs $1M + 3M_c$ and
$Z_{3n} \leftarrow Z_n$
$[(-3c^2 d^2)J - d(c^4 d + 1)N - (\frac{3}{2}c^2 d)H + (c^2)K]$
which costs $1M + 2M_c$. In the above, once $(c^2)K$ is computed, the cost of computing $(3c^2)K$ is ignored. The complexity of the new algorithm is $(10S + 2M + 5M_c)$. If $3S < 2M + 3M_c$, then the new

complexity of $(10S + 2M + 5M_c)$ is less than the older complexity of $(7S+4M+8M_c)$. In (Bernstein, 2006a), $2M = 3S$ and thus $3S < 2M + 3M_c$.

**DD. SQO Doubling for Generalised Edwards Coordinates:**
By inspecting formula(D) in Section 2 and taking into consideration that we are provided with $X_{2n}^2$ and $Y_{2n}^2$, we can see that the total complexity of the formula(D) is $(5S+5M_c)$. We can improve upon this. Using the doubling formula(BB) in this section, we can write

$$Y_{2n}^2 = \left[2Y_n^2Z_n^2 - c^2(Z_n^4 + dY_n^4)\right]^2$$
$$Z_{2n}^2 = \left[-c^2d(2Y_n^2Z_n^2) + (Z_n^4 + dY_n^4)\right]^2$$

Given that only squares of the coordinates are stored, the above formula can be computed using the following algorithm:

| | | |
|---|---|---|
| $A \leftarrow (Y_n^2)^2$ | $(= Y_n^4)$ | $1S$ |
| $B \leftarrow (Z_n^2)^2$ | $(= Z_n^4)$ | $1S$ |
| $E \leftarrow (Y_n^2 + Z_n^2)^2 - A - B$ | $(= 2Y_n^2Z_n^2)$ | $1S$ |
| $Y_{2n}^2 \leftarrow [E -$ $c^2(B+dA)]^2$ | $(= [2Y_n^2Z_n^2$ $-c^2(Z_n^4 + dY_n^4)]^2$ | $1S+2M_c$ |
| $Z_{2n}^2 \leftarrow [-c^2dE +$ $(B+dA)^2]^2$ | $(= [-c^2d(2Y_n^2Z_n^2)$ $+(Z_n^4 + dY_n^4)]^2$ | $1S+M_c$ |

The complexity of the new algorithm is $(5S + 3M_c)$ while the older complexity was $(5S+5M_c)$

**EE. SQO Tripling for Generalised Edwards Coordinates:**
By inspecting formula(E) in Section 2, we can see that the total complexity of formula(E) is $(4M+7S+8M_c)$. The algorithm used to compute $Y_{3n}$ and $Z_{3n}$ in formula(CC) of this section can be adapted to compute the requisite formulae. The first two steps can be omitted as squares are already available and the last two steps can be replaced with

$$Y_{3n}^2 \leftarrow Y_n^2\left[(c^2d^2)J - (\frac{3}{2}c^2d)H + (c^2d+1)M - (3c^2)K\right]^2$$
$$Z_{3n}^2 \leftarrow Z_n^2\left[(-3c^2d^2)J - d(c^4d+1)N - (\frac{3}{2}c^2d)H + (c^2)K\right]^2$$

The complexity of this algorithm would be the same as that of formula(CC) which is $(10S+2M+5M_c)$. We can take $2M = 3S$ (Bernstein, 2006a). Thus $3S < (2M + 3M_c)$ and the new algorithm with complexity $(10S + 2M + 5M_c)$ is better than the older one with complexity $(7S+4M+8M_c)$.

**FF. Affine $w$-coordinate Differential Addition and Doubling for a new model of Binary Edwards Curves proposed in (H.Wu et al., 2012):**
The operation count of computing $w_4$ in formula (F) in Section 2 is $1I+1M+1M_c+2S$ as the formula can be computed using the algorithm below:

| | | |
|---|---|---|
| $A = w_2^2$ | $(= w_2^2)$ | $1S$ |
| $B = A^2$ | $(= w_2^4)$ | $1S$ |
| $C = t^2A$ | $(= t^2w_2^2)$ | $1M_c$ |
| $D = C^{-1}$ | $\left(= \frac{1}{t^2w_2^2}\right)$ | $1I$ |
| $w_4 = (1+B)D$ | $\left(= \frac{1+w_2^4}{t^2w_2^2}\right)$ | $1M$ |

Now $w_4$ can be rewritten as

$$w_4 = \left(\frac{1}{t^2}\right)\left(\frac{1}{w_2^2} + w_2^2\right) \text{ and}$$

$w_4$ can be computed using the following algorithm:

| | | |
|---|---|---|
| $A = w_2^2$ | $(= w_2^2)$ | $1S$ |
| $B = \frac{1}{A}$ | $\left(= \frac{1}{w_2^2}\right)$ | $1I$ |
| $w_4 = \left(\frac{1}{t^2}\right)(A+B)$ | $\left(= \left(\frac{1}{t^2}\right)\left(\frac{1}{w_2^2} + w_2^2\right)\right)$ | $M_c$ |

Thus the complexity of the new doubling algorithm is $1I + 1S + 1M_c$ resulting in a saving of $1M + 1S$. The formulae(F) for differential addition($w_5$) in the previous section costs $1I + 2M + 2S + 1M_c$. Considering that $w_2^2$ is computed both in the differential addition and doubling steps, $w_2^2$ can be computed just once. Thus the new total cost of a differential addition and doubling is $2I + 2M + 2S + 2M_c$ or $1I + 5M + 2S + 2M_c$ with Montgomery's Inversion trick, as compared to the previous total cost of $1I + 6M + 4S + 2M_c$ resulting in an overall saving of $1M + 2S$.

# 4 DOUBLING IN TWISTED EDWARDS CURVES

In this section, we look at the doubling formula for Twisted Edwards Curves with a particular parameterization and then propose alternate formulae for the same. Building on the work of Edwards(Edwards, 2007), the authors in (Bernstein et al., 2008b) introduced Twisted Edwards Curves, whose equation is given by

$$ax^2 + y^2 = 1 + dx^2y^2 \quad (2)$$

where $K$ is a field of odd characteristic $a,d \in K$ with $ad(a-d) \neq 0$. Here, we closely follow the treatment in (Hisil, 2010), where, amongst others, the formulae for Homogeneous Projective, Inverted and Extended Homogeneous Projective coordinates are presented. The triplet $(X : Y : Z)$ satisfies the homogeneous projective equation $aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2$.

**Homogenous Projective Coordinates:**
Here the triplet $(X : Y : Z)$ corresponds to the affine point $(X/Z, Y/Z)$ with $Z \neq 0$. If $P = (X_1 : Y_1 : Z_1)$ then the doubling formula for $[2]P = (X_2 : Y_2 : Z_2)$ is as below: (assuming $Z_2 \neq 0$).

$$X_2 = 2X_1Y_1(2Z_1^2 - Y_1^2 - aX_1^2)$$
$$Y_2 = (Y_1^2 - aX_1^2)(Y_1^2 + aX_1^2)$$
$$Z_2 = (Y_1^2 + aX_1^2)(2Z_1^2 - Y_1^2 - aX_1^2)$$

Evaluating the above doubling formulae as in (Bernstein et al., 2008b) costs $3M + 4S + 1M_c$ and is computed using the following algorithm:

| | | |
|---|---|---|
| $B \leftarrow (X_1 + Y_1)^2$ | $(= X_1^2 + Y_1^2 + 2X_1Y_1)$ | $S$ |
| $C \leftarrow X_1^2$ | $(= X_1^2)$ | $S$ |
| $D \leftarrow Y_1^2$ | $(= Y_1^2)$ | $S$ |
| $E \leftarrow aC$ | $(= aX_1^2)$ | $M_c$ |
| $F \leftarrow E + D$ | $(= Y_1^2 + aX_1^2)$ | |
| $H \leftarrow Z_1^2$ | $(= Z_1^2)$ | $S$ |
| $J \leftarrow F - 2H$ | $(= -(2Z_1^2 - Y_1^2 - aX_1^2))$ | |
| $X_2 \leftarrow (B - C - D)J$ | $(= -(2X_1Y_1)$ $(2Z_1^2 - Y_1^2 - aX_1^2))$ | $M$ |
| $Y_2 \leftarrow F(E - D)$ | $(= -(Y_1^2 - aX_1^2)$ $(Y_1^2 + aX_1^2))$ | $M$ |
| $Z_2 \leftarrow -FJ$ | $(= (Y_1^2 + aX_1^2)$ $(2Z_1^2 - Y_1^2 - aX_1^2))$ | $M$ |

If $a = 1$, then the doubling costs $3M + 4S$ by replacing the instruction $X_2 \leftarrow (B - C - D)J$ in the above algorithm with $X_2 \leftarrow (B - F)J$, as in (Bernstein and T.Lange, 2007a).
If $a = -1$, then the doubling again costs $3M + 4S$ and can be computed using the following algorithm as provided in (Hisil, 2010):

| | | |
|---|---|---|
| $A \leftarrow 2Z_1^2$ | $(= 2Z_1^2)$ | $S$ |
| $B \leftarrow Y_1^2$ | $(= Y_1^2)$ | $S$ |
| $C \leftarrow X_1^2$ | $(= X_1^2)$ | $S$ |
| $D \leftarrow B + C$ | $(= X_1^2 + Y_1^2)$ | |
| $E \leftarrow B - C$ | $(= Y_1^2 - X_1^2)$ | |
| $F \leftarrow A - E$ | $(= 2Z_1^2 + X_1^2 - Y_1^2)$ | |
| $X_2 \leftarrow ((X_1 + Y_1)^2 - D)F$ | $(= (2X_1Y_1)$ $(2Z_1^2 + X_1^2 - Y_1^2))$ | $S + M$ |
| $Y_2 \leftarrow DE$ | $(= (X_1^2 + Y_1^2)$ $(Y_1^2 - X_1^2))$ | $M$ |
| $Z_2 \leftarrow EF$ | $(= (Y_1^2 - X_1^2)$ $(2Z_1^2 + X_1^2 - Y_1^2))$ | $M$ |

**Inverted Coordinates:**
Here the triplet $(X : Y : Z)$ corresponds to the affine point $(Z/X, Z/Y)$ with $Z \neq 0$. If the triplet $(X_1 : Y_1 : Z_1)$ satisfies the homogeneous projective equation $aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2$ and $X_1Y_1Z_1 \neq 0$, then the doubling formulae for $[2]P = (X_2 : Y_2 : Z_2)$ is as below: (assuming $X_2Y_2Z_2 \neq 0$):

$$X_2 = (X_1^2 - aY_1^2)(X_1^2 + aY_1^2)$$
$$Y_2 = 2X_1Y_1(X_1^2 + aY_1^2 - 2dZ_1^2)$$
$$Z_2 = 2X_1Y_1(X_1^2 - aY_1^2)$$

Evaluating the above doubling formulae as in (Bernstein et al., 2008b) costs $3M + 4S + 2M_c$ and is computed using the following algorithm:

| | | |
|---|---|---|
| $A \leftarrow X_1^2$ | $(= X_1^2)$ | $S$ |
| $B \leftarrow Y_1^2$ | $(= Y_1^2)$ | $S$ |
| $U \leftarrow aB$ | $(= aY_1^2)$ | $M_c$ |
| $C \leftarrow A + U$ | $(= (X_1^2 + aY_1^2))$ | |
| $D \leftarrow A - U$ | $(= (X_1^2 - aY_1^2))$ | |
| $E \leftarrow (X_1 + Y_1)^2 - A - B$ | $(= 2X_1Y_1)$ | $S$ |
| $X_2 \leftarrow CD$ | $(= (X_1^2 + aY_1^2)(X_1^2 - aY_1^2))$ | $M$ |
| $Y_2 \leftarrow E(C - (2d)Z_1^2)$ | $(= 2X_1Y_1$ $(X_1^2 + aY_1^2 - 2dZ_1^2))$ | $M + M_c + S$ |
| $Z_2 \leftarrow DE$ | $(= 2X_1Y_1(X_1^2 - aY_1^2))$ | $M$ |

If $a = 1$ then the doubling takes $3M + 4S + 1M_c$ by computing $E$ as $(X_1 + Y_1)^2 - C$ see (Bernstein and T.Lange, 2007b).
If $a = -1$ then the doubling again takes $3M + 4S + 1M_c$ by computing $E$ as $(X_1 + Y_1)^2 - D$ and replacing $U \leftarrow aB$, $C \leftarrow A + U$, $D \leftarrow A - U$ with $C \leftarrow A - B$, $D \leftarrow A + B$ as given in (Hisil, 2010).

**Extended Homogenous Projective Coordinates:**
In this system, each point $(x,y)$ on $ax^2 + y^2 = 1 + dx^2y^2$ is represented by the quadruplet $(X : Y : T : Z)$ which in turn corresponds to the affine point $(X/Z, Y/Z)$ with the auxiliary coordinate $T = XY/Z$ and $Z \neq 0$. If $(X_1 : Y_1 : T_1 : Z_1)$ with $Z_1 \neq 0$ and

$T_1 = X_1Y_1/Z_1$ satisfy $aX^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2$, then the doubling formulae for $[2](X_1, Y_1, T_1, Z_1) = (X_2 : Y_2 : T_2 : Z_2)$ is as follows (assuming $Z_2 \neq 0$):

$$X_2 = 2X_1Y_1(2Z_1^2 - Y_1^2 - aX_1^2)$$
$$Y_2 = (Y_1^2 - aX_1^2)(Y_1^2 + aX_1^2)$$
$$T_2 = 2X_1Y_1(Y_1^2 - aX_1^2)$$
$$Z_2 = (Y_1^2 + aX_1^2)(2Z_1^2 - Y_1^2 - aX_1^2)$$

Evaluating the above doubling formulae as in (Hisil, 2010) costs $4M + 4S + 1M_c$ and is computed using the following algorithm:

| | | |
|---|---|---|
| $A \leftarrow X_1^2$ | $(= X_1^2)$ | $S$ |
| $B \leftarrow Y_1^2$ | $(= Y_1^2)$ | $S$ |
| $C \leftarrow 2Z_1^2$ | $(= 2Z_1^2)$ | $S$ |
| $D \leftarrow aA$ | $(= aX_1^2)$ | $M_c$ |
| $E \leftarrow B + D$ | $(= Y_1^2 + aX_1^2)$ | |
| $F \leftarrow B - D$ | $(= Y_1^2 - aX_1^2)$ | |
| $G \leftarrow C - E$ | $(= 2Z_1^2 - (Y_1^2 + aX_1^2))$ | |
| $H \leftarrow (X_1 + Y_1)^2$ $-A-B$ | $(= 2X_1Y_1)$ | $S$ |
| $X_2 \leftarrow GH$ | $(= (2X_1Y_1)$ $(2Z_1^2 - Y_1^2 - aX_1^2))$ | $M$ |
| $Y_2 \leftarrow EF$ | $(= (Y_1^2 - aX_1^2)$ $(Y_1^2 + aX_1^2))$ | $M$ |
| $T_2 \leftarrow FH$ | $(= 2X_1Y_1(Y_1^2 - aX_1^2))$ | $M$ |
| $Z_2 \leftarrow EG$ | $(= (Y_1^2 + aX_1^2)$ $(2Z_1^2 - Y_1^2 - aX_1^2))$ | $M$ |

If $a = 1$ then the doubling costs $4M + 4S$ and can be computed by first removing $D \leftarrow aA$ and then replacing $E \leftarrow B + D$, $F \leftarrow B - D$, $H \leftarrow (X_1 + Y_1)^2 - A - B$ with $E \leftarrow B + A$, $F \leftarrow B - A$, $H \leftarrow (X_1 + Y_1)^2 - E$, respectively.
If $a = -1$ then the doubling costs $4M + 4S$ and can be computed by first removing $D \leftarrow aA$ and then replacing $E \leftarrow B + D$, $F \leftarrow B - D$, $H \leftarrow (X_1 + Y_1)^2 - A - B$ with $E \leftarrow B - A$, $F \leftarrow B + A$, $H \leftarrow (X_1 + Y_1)^2 - F$, respectively.

**New Alternate Algorithm to Compute Doubling Formulae for Homogeneous Projective, Inverted and Extended Homogeneous Projective Coordinates ($a = 1$ or $a = -1$):**
Here we provide an alternate algorithm to compute a doubling on Twisted Edwards Curves. It is possible to collect instructions that are common to all the 3 computations, compute them separately and then perform computations that are specific to the coordinate system being used. Below, we first present instructions that are common to all the 3 coordinate systems considered here and then present instructions that are specific to the coordinate system being used. We note here that for all nonzero $c \in \overline{K}$, $(X : Y : Z) = (cX : cY : cZ)$.

**Instructions Common to all 3 Coordinate Systems:**

| | | |
|---|---|---|
| $A \leftarrow (X_1 + Y_1)^2$ | $(= X_1^2 + Y_1^2 + 2X_1Y_1)$ | $S$ |
| $B \leftarrow (X_1 - Y_1)^2$ | $(= X_1^2 + Y_1^2 - 2X_1Y_1)$ | $S$ |
| $C \leftarrow A + B$ | $(= 2(X_1^2 + Y_1^2))$ | |
| $D \leftarrow A - B$ | $(= 4X_1Y_1)$ | |
| $E \leftarrow (Z_1 + Z_1)^2$ | $(= 4Z_1^2)$ | $S$ |
| $F \leftarrow (X_1 + X_1)^2$ | $(= 4X_1^2)$ | $S$ |
| $G \leftarrow C - F$ | $(= 2(Y_1^2 - X_1^2))$ | |

**Instructions Specific to Homogenous Projective Coordinates:**

| | | |
|---|---|---|
| $Y_2 \leftarrow CG$ | $(= 4(Y_1^2 + X_1^2)(Y_1^2 - X_1^2))$ | $M$ |
| if $a = +1$ | | |
| $X_2 \leftarrow D(E - C)$ | $(= (4X_1Y_1)(4Z_1^2 - 2(X_1^2 + Y_1^2)))$ | $M$ |
| $Z_2 \leftarrow C(E - C)$ | $(= 2(X_1^2 + Y_1^2)$ $(4Z_1^2 - 2(X_1^2 + Y_1^2)))$ | $M$ |
| if $a = -1$ | | |
| $X_2 \leftarrow D(E - G)$ | $(= (4X_1Y_1)(4Z_1^2 - 2(Y_1^2 - X_1^2)))$ | $M$ |
| $Z_2 \leftarrow G(E - G)$ | $(= (2(Y_1^2 - X_1^2)))$ $(4Z_1^2 - 2(Y_1^2 - X_1^2))$ | $M$ |

**Instructions Specific to Inverted Coordinates:**

| | | |
|---|---|---|
| $X_2 \leftarrow CG$ | $(= 4(Y_1^2 + X_1^2)(Y_1^2 - X_1^2))$ | $M$ |
| if $a = +1$ | | |
| $Y_2 \leftarrow D(dE - C)$ | $(= (4X_1Y_1)(4dZ_1^2 - 2(X_1^2 + Y_1^2))$ | $M$ |
| $Z_2 \leftarrow DG$ | $(= (4X_1Y_1)(2(Y_1^2 - X_1^2)))$ | $M$ |
| if $a = -1$ | | |
| $Y_2 \leftarrow D(dE + G)$ | $(= (4X_1Y_1)(4dZ_1^2 + 2(Y_1^2 - X_1^2)))$ | $M$ |
| $Z_2 \leftarrow -DC$ | $(= (-4X_1Y_1)(2(X_1^2 + Y_1^2)))$ | $M$ |

**Instructions Specific to Extended Homogenous Projective Coordinates:**

| | | |
|---|---|---|
| $Y_2 \leftarrow CG$ | $(= 4(X_1^2 + Y_1^2)(Y_1^2 - X_1^2))$ | $M$ |
| if $a = +1$ | | |
| $X_2 \leftarrow D(E - C)$ | $(= (4X_1Y_1)(4Z_1^2 - 2(X_1^2 + Y_1^2)))$ | $M$ |
| $T_2 \leftarrow DG$ | $(= (4X_1Y_1)(2(Y_1^2 - X_1^2)))$ | $M$ |
| $Z_2 \leftarrow C(E - C)$ | $(= (2(X_1^2 + Y_1^2))$ $(4Z_1^2 - 2(X_1^2 + Y_1^2)))$ | $M$ |
| if $a = -1$ | | |

$$X_2 \leftarrow D(E-G) \quad (=(4X_1Y_1)(4Z_1^2-2(Y_1^2-X_1^2))) \quad M$$
$$T_2 \leftarrow DC \quad (=(4X_1Y_1)(2(X_1^2+Y_1^2))) \quad M$$
$$Z_2 \leftarrow G(E-G) \quad (=(2(Y_1^2-X_1^2)) \quad M$$
$$(4Z_1^2-2(Y_1^2-X_1^2)))$$

The cost of the new algorithm presented here is the same as that of the currently known best algorithms in the literature due to Bernstein and Hisil depicted above (i.e., $3M+4S$ operations each for Homogeneous Projective and Inverted coordinates and $4S+4M$ operations for Extended Homogeneous Projective coordinates when the curve parameter $a=1$ or $-1$). However, in the new algorithm, the non-coordinate specific instructions can be separated from the coordinate specific instructions as shown above(variables $A \ldots G$ are common to all coordinate forms) and further within each coordinate system, one instruction is independent of whether $a=1$ or $-1$. Thus the new algorithm's footprint may be lower than the sum of the footprints of currently known algorithms for the three coordinate systems under consideration. Thus the new algorithm may be an attractive alternative when the implementation is intended to work across the three coordinate systems, namely Homogeneous Projective, Inverted and Extended Homogeneous Projective Coordinates.

# 5 CONCLUSION

In this paper, we improved the arithmetic for differential addition on Generalized Edwards curves. We also improved the $w$-coordinate formulae for a new model of elliptic curve proposed by Wu, Tang and Feng. We also provided a new algorithm for point doubling on Twisted Edwards Curves with a lower foot print for implementation.

# ACKNOWLEDGEMENTS

The author would like to sincerely thank the anonymous reviewers of SECRYPT 2016 for their extremely useful comments and suggestions.

# REFERENCES

Bernstein, D. (2006a). Curve25519: New Diffie-Hellman speed records. In *Public Key Cryptography - PKC 2006*, LNCS 3958.

Bernstein, D. (2006b). Differential Addition Chains. Technical report, http://cr.yp.to/ecdh/diffchain-20060219.pdf accessed on 30th Nov 2015.

Bernstein, D. and Lange, T. (2007). Explicit Forms Database(EFD). Technical report, http://hyperelliptic.org/EFD/ accessed on 30th Nov 2015.

Bernstein, D., Lange, T., and Farashahi, T. (2008a). Binary Edwards Curves. In *Cryptographic Hardware and Embedded Systems - CHES 2008*, LNCS 5154.

Bernstein, D., P.Birkner, M.Joye, T.Lange, and C.Peters (2008b). Twisted Edwards Curves. In *AFRICACRYPT 2008*, LNCS 5023.

Bernstein, D. and T.Lange (2007a). Faster addition and doubling on Elliptic curves. In *ASIACRYPT 2007*, LNCS 4833.

Bernstein, D. and T.Lange (2007b). Inverted Edwards coordinates. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-17*, LNCS 4851.

D.Knuth (1998). *The Art of Computer Programming Vol 2*. Pearson Education.

E.Brier and M.Joye (2002). Weierstrass Elliptic Curves and side channel attacks. In *Public Key Cryptography - PKC 2002*, LNCS 2274.

Edwards, H. (2007). A normal form for elliptic curves. *Bulletin of the AMS*, 44(3):393422.

Hisil, H. (2010). *Elliptic Curves,Group Law, and Efficient Computation*. PhD thesis, Queensland University of Technology.

H.Wu, C.Tang, and R.Feng (2012). A new model of Binary Elliptic Curves. In *INDOCRYPT 2012*, LNCS 7668.

J.Lopez and R.Dahab (1999). Fast multiplication on Elliptic Curves over $GF(2^m)$ without precomputation. In *Cryptographic Hardware and Embedded Systems - CHES 1999*, LNCS 1717.

M.Joye and S.Yen (2002). The Montgomery Powering Ladder. In *Cryptographic Hardware and Embedded Systems - CHES 2002*, LNCS 2523.

Montgomery, P. L. (1992). Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains. Technical report, ftp://ftp.cwi.nl/pub/pmontgom/Lucas.ps.gz accessed on 30th Nov 2015.

P.L.Montgomery (1987). Speeding the Pollard and Elliptic Curve methods of Factorization. In *Mathematics of Computation Vol 48, Issue 177 Jan 1987*.

R.Justus and Loebenberger, D. (2010). Differential Addition in Generalized Edwards Coordinates. In *5th International Workshop on Security - IWSEC 2010,*, LNCS 6434.