**Pure and Applied Mathematics Journal**
2025; 14(5): 135-156
http://www.sciencepublishinggroup.com/j/pamj
doi: 10.11648/j.pamj.20251405.15

# Same Values Analysis Attack over Binary Elliptic Curves

**Aubain Jose Mayeukeu[1, *], Emmanuel Fouotsa[2], Celestin Lele[1]**

[1]Departement of Mathematics and Computers Sciences, University of Dschang, Dschang, Cameroon
[2]Center of Cybersecurity and Mathematical Cryptology, the University of Bamenda, Bambili, Cameroon

## Email address:

mayeukeuaubainjose@gmail.com (Aubain Jose Mayeukeu), emmanuelfouotsa@yahoo.fr (Emmanuel Fouotsa), celestinlele@yahoo.fr (Celestin Lele)
[*]Corresponding author

## To cite this article:

Aubain Jose Mayeukeu, Emmanuel Fouotsa, Celestin Lele. (2025). Same Values Analysis Attack over Binary Elliptic Curves. *Pure and Applied Mathematics Journal, 14*(5), 135-156. https://doi.org/10.11648/j.pamj.20251405.15

**Received:** 6 August 2025; **Accepted:** 21 August 2025; **Published:** 22 October 2025

**Abstract:** In this work, we are interested in studying a particular class of Side Channel Attacks on elliptic curves defined over binary fields. Side Channel Attacks exploit physical leakages such as power consumption or electromagnetic emanations during cryptographic computations in order to recover secret information. Among these attacks, the one we focus on is known as *Same Values Analysis (SVA)*. This method does not rely directly on distinguishing the sequence of operations, but rather on detecting situations where different inputs lead to identical intermediate values inside the formulas used for point addition and point doubling. Since these formulas are usually well known and publicly available, an adversary can exploit such collisions in order to reveal sensitive information, in particular the secret scalar used during scalar multiplication. The objective of our study is therefore to identify the points on elliptic curves that produce identical intermediate variables during addition or doubling steps, and to determine the algebraic conditions under which such coincidences occur. By analyzing these conditions, one can highlight vulnerabilities in scalar multiplication algorithms and evaluate their potential exploitation. We will focus our investigation on three important families of elliptic curves over binary fields: *Weierstrass curves, Edwards curves, and Hessian curves*. For completeness, we will also verify the effectiveness of the SVA attack on standardized curves recommended by NIST and SECG. The results of our analysis clearly show that all these curves are vulnerable to Same Values Analysis, which implies that their use in cryptographic protocols requires a careful reassessment of security guarantees.

**Keywords:** Elliptic Curve Cryptography, Side Channel Attack, Same Values Analysis, Hessian Curve, Edwards Curve

## 1. Introduction

Elliptic curve cryptography (ECC) was introduced towards the end of the 20th century, specifically in 1985 by V. Miller [1] and 1987 N. Koblitz [2]. It has become so widespread and is increasingly recommended due to its major advantage: it offers very small key sizes compared to other methods. However, ECC is increasingly subject to several auxiliary key attacks. The simplest of which is Simple Power Analysis (SPA), which simply observes a single trace of current consumption during the implementation of the scalar multiplication algorithm and focuses on the difference in consumption between an addition and a doubling of points. An attacker who would be able to make this distinction could effectively identify the bits of the secret key [3]. By using the binary method for scalar multiplication, the attack could be applied to elliptic curves cryptosystems. The simplest way to counter this attack would be to use methods that always perform additions and doubling of points regardless of the key bit. We can thus speak of the Binary method and the double and add always method. Even with this method, elliptic curve cryptosystems are vulnerable to more serious attacks called Differential Power Analysis (DPA) [3]. DPA can be prevented by using randomization countermeasures such as point randomization [4], curve randomization [5].

These randomization methods are ineffective on points with zero coordinates, it is this observation that motivated Goubin to propose an attack based on points with zero coordinates: this is the Refined Power Analysis (RPA) [6]. Smart proposed isogeny defense as an effective countermeasure

against RPA[7]. However, the absence of these points with zero coordinates on several curves motivated Akishita and T.Takagi to extend the RPA by focusing this time on points which admit at least one zero intermediate value during the addition or doubling of points: this is the Zero Value Point ( ZVP) attack [8]. The ZVP appears to be a very effective attack and the majority of the recommended curves are vulnerable to this attack. The improvement of the smart countermeasure by Akishita and T.Takagi [8] allowed them to propose isogeny defense as a countermeasure of the ZVP. C. Crepeau and R. Kazmi[9] studied the ZVP on elliptic curves defined over binary fields and noted that some recommended curves by the National Institute of Standards and Technology (NIST) and the Standards for Efficient Cryptography Group (SECG) are resistant to attack.

Cédric Murdica *et al.* [10] looked at the intermediate values in more detail and proposed an essentially linked attack on equal intermediate values. Among these identical intermediate values, they searched for those that would cause a collision when implementing the scalar multiplication algorithm. Their work was focused on Weierstrass curve over primary fields Martinez *et al.* [11] studied Same Values Analysis on Edwards curve over primary fields.

Elliptic curve arithmetic defined on binary fields is very efficient and easier, international standardization companies such as NIST and SECG have also published a list of highly recommended binary curves in cryptography, which motivates the interest in studying the vulnerability of these curves on the SVA attack

In addition to the classical studies on Same Values Analysis (SVA) and other side-channel attacks on elliptic curve cryptography, several recent works (2023–2025) have highlighted new vulnerabilities, both in ECC and in post-quantum cryptography (PQC).

1. *Battistello et al. (2025)* proposed a novel approach based on Long Short-Term Memory (LSTM) neural networks to analyze power traces and recognize patterns of elliptic curve operations. Their results demonstrate that, even when countermeasures such as coordinate randomization are applied, side-channel collisions can still be identified, leading to partial recovery of secret scalars [12].
2. *Cintas Canto et al. (2023)* provided a comprehensive survey entitled *Algorithmic Security is Insufficient*, which reviews physical and side-channel attacks on post-quantum candidates. Their conclusion is that theoretical (algorithmic) security is not sufficient if implementations are physically vulnerable [13].
3. Several recent *IACR ePrint reports (2023–2024)* introduced new side-channel and fault-injection attacks against post-quantum key encapsulation mechanisms, such as *Crystals-Kyber* and *HQC*. These works demonstrate that chosen-ciphertext assisted side-channel attacks can exploit ciphertext validity checks to break implementations [14].
4. Finally, a *2023 roadmap on PQC standardization* emphasized that side-channel resilience must be treated as a first-class requirement in the NIST post-quantum cryptography process, presenting a taxonomy of attacks and countermeasures relevant to PQC and ECC implementations alike [15].

In this work, we are interested in the study of the SVA attack on all binary curve models, notably the Weierstrass curve, Edwards curve and Hessian curve. We look at the effectiveness of this attack on the recommended binary curves for this we use the computer algebra system SageMath. We want to point out that this article is an extension of our work published at the 15th International Cryptography Conference for Africa (Africacrypt 2024). In this previous work, we were only interested in Weierstrass curves, but here we generalize the study to the three curve models. These contributions confirm that side-channel vulnerabilities remain critical, not only for classical elliptic curves but also for post-quantum primitives. They highlight the necessity of incorporating robust countermeasures at the implementation level, beyond algorithmic guarantees.

The work is organized as follows: in Section 2, we review the important concepts on binary curves, notably the different formulas useful for scalar multiplication. In Section 3, we study SVA on binary curves, in Section 4, we are interested in this attack on recommended curves and in Section 5, we give our conclusion.

# 2. Binary Elliptic Curve and Scalar Multiplication

We make sure to first give the important notions on elliptic curves over binary fields. Throughout this work, $\mathbb{K}$ denotes the binary field $\mathbb{F}_{2^m}$ where $m$ is a positive interger

## *2.1. Binary Elliptic Curve in Affine Coordinates*

In this part, we recall the formulas for point addition and doubling in affine coordinates. We begin with the case of Weierstrass curves.

### *2.1.1. Weiestrass Binary Curve*

Over a binary fields $K$ the Weierstrass form of ellictic curve is described as

$$E : y^2 + xy = x^3 + Ax^2 + B, \quad (A, B \in \mathbb{K}).$$

We can define a group law on the set of points of an elliptic curve in the following way: the opposite of a point $P = (x, y)$ is the point $-P = (x, x + y)$ [16] and the neutral element for this law is a particular point called point at infinity. the sum of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, is the point $P_3 = P_1 + P_2 = (x_3, y_3)$ compute as follows:

1. If $P_1 \neq \pm P_2$, then

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right) + \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 + A,$$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_2 + A + 1) + \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^3 + x_1 + x_2 + A + y_1.$$

2. If $P_1 = P_2$, then

$$x_3 = \left(\frac{x_1 + y_1}{x_1}\right) + \left(\frac{x_1 + y_1}{x_1}\right)^2 + A,$$

$$y_3 = \left(\frac{x_1 + y_1}{x_1}\right)(x_1 + A + 1) + \left(\frac{x_1 + y_1}{x_1}\right)^3 + A + y_1.$$

These formulas can be found in [16].

#### 2.1.2. Edwards Binary Curve

Let $d_1, d_2 \in \mathbb{K}$ such that $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The binary Edwards curve with the coefficients $d_1, d_2$ is the affine curve:

$$E : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$$

If $(x, y) \in E$ then $(y, x) \in E$ and $-(x, y) = (y, x)$. The neutral element for the addition law is the point $(0, 0)$.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the binary curve $E$ and $P_3 = (x_3, y_3) = P_1 + P_2$. $P_3$ is computed as follows:

1. If $P_1 \neq \pm P_2$, then
   $x_3 = \frac{d_1(x_1+x_2)+d_2(x_1+y_1)(x_2+y_2)+(x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)}$ $\quad y_3 = \frac{d_1(y_1+y_2)+d_2(x_1+y_1)(x_2+y_2)+(y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1+(y_1+y_1^2)(x_2+y_2)}$.
2. If $P_1 = P_2$ then
   $x_3 = 1 + \frac{d_1(1+x_1+y_1)}{d_1+x_1y_1+x_1^2(1+x_1+y_1)}$ $\quad y_3 = 1 + \frac{d_1(1+x_1+y_1)}{d_1+x_1y_1+y_1^2(1+x_1+y_1)}$.

These formulas can be found in [16].

#### 2.1.3. Binary Hessian Curves

Let $d \in \mathbb{K}$. The binary Hessian curve with the coefficients $d$ is the affine curve:

$$E : x^3 + y^3 + 1 = 3dxy$$

If $(x, y) \in E$ then $(y, x) \in E$ and $-(x, y) = (y, x)$.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the binary Hessian curve $E$ and $P_3 = (x_3, y_3) = P_1 + P_2$. $P_3$ is computed as follows:

1. If $P_1 \neq \pm P_2$, then

$$x_3 = \frac{x_2y_1^2 - x_1y_2^2}{x_2y_2 - x_1y_1}$$

.

$$y_3 = \frac{y_2x_1^2 - y_1x_2^2}{x_2y_2 - x_1y_1}$$

.

2. If $P_1 = P_2$ then

$$x_3 = \frac{y_1(1 - x_1^3)}{x_1^3 - y_1^3}$$

$$y_3 = \frac{x_1(y_1^3 - 1)}{x_1^3 - y_1^3}$$

These different affine addition formulas involve field inversions, which are computationally expensive. To avoid such inversions, it is recommended to use alternative coordinate systems, such as projective coordinates.

### 2.2. Binary Curve and Projective Coordinates

#### 2.2.1. Weierstrass Binary Curve in Projective Coordinates

In the database of explicit formulas [16], several formulas have been proposed for the addition of points in projective coordinates on binary Weierstrass curves. Among these different formulas, the most efficient ones [17] by J. Lopez and R. Dahab. Here, to pass from affine coordinates $(x, y)$ to projective coordinates $(X, Y, Z)$, the authors perform the transformation $x = X/Z$ and $y = Y/Z^2$ [9]. Let $add^{\mathcal{P}}(P_1; P_2)$ and $dbl^{\mathcal{P}}(P_1)$ denote respectively the addition point and de point doubling in affine coordinates. The point $P_3 = P_1 + P_2$ is obtained by:

1. $P_3 = add^{\mathcal{P}}(P_1, P_2)$
   with $X_3 = H + G + C^2$, $Y_3 = IH + JZ_3$, $Z_3 = F^2$, where:
   $A_0 = Z_1^2Y_2$,$A_1 = Z_2^2Y_1$, $B_0 = Z_1X_2$, $B_1 = Z_2X_1$, $C = A_1 + A_0$, $D = B_1 + B_0$, $E = Z_2Z_1$, $F = ED$, $G = (AE^2 + F)D^2$, $H = FC$, $I = X_3 + B_0ED^2$, $J = X_3 + A_0D^2$
2. $P_3 = dbl^{\mathcal{P}}(P_1)$
   $Z_3 = X_1^2Z_1^2$, $X_3 = BZ_1^4 + X_1^4$, $Y_3 = X.(AZ_3 + Y_1^2 + BZ_1^4) + BZ_1^4Z_3$

in the explicit for of $add^{\mathcal{P}}(P_1, P_2)$ and $dbl^{\mathcal{P}}(P_1)$ are given below. In these different algorithms, the calculation of intermediate values as well as the operations on the degrees of their Z coordinate are explicitly presented

Let $P_1 = (Z_1x_1 : Z_1^2y_1 : Z_1)$ and $P_2 = (Z_2x_2 : Z_2^2y_2 : Z_2)$ for some $Z_1, Z_2 \in \mathbb{K}$ and $P_3 = add^{\mathcal{P}}(P_1; P_2)$ in case of point addition on Projective coordinates over binary fields and $P_3 = dbl^{\mathcal{P}}(P_1)$ point doubling on Projective coordinates over binary fields [9, 18].

***Table 1.*** *Doubling over Weierstrass Binary Curve.*

| **Algorithm: dbl**$^{\mathcal{P}}$ over Weierstrass Binary Curves [9, 18] | | | |
|---|---|---|---|
| **Input**: $(P_1 \neq \mathcal{O},\ c = B^{2^{m-1}})$ | | | |
| **Output**: $P_3 = (X_3, Y_3, Z_3) = 2P_1$ | | | |
| | **Operation** | **Intermediate Values Computed** | $\mathbf{deg(Z_1)}$ |
| 1 | $R_1 \leftarrow X_1, \quad R_2 \leftarrow Y_1,$ | | |
| | $R_3 \leftarrow Z_1$ | | |
| 2 | $R_4 \leftarrow c$ | | |
| 3 | $R_3 \leftarrow R_3 \times R_3$: | $\{= Z_1^2 = D_1\}$ | $(2 \leftarrow 1 \times 1)$ |
| 4 | $R_4 \leftarrow R_3 \times R_4$: | $\{= Z_1^2 c = D_2\}$ | $(2 \leftarrow 0 \times 2)$ |
| 5 | $R_4 \leftarrow R_4 \times R_4$: | $\{= Z_1^4 B = D_4\}$ | $(4 \leftarrow 2 \times 2)$ |
| 6 | $R_1 \leftarrow R_1 \times R_1$: | $\{= X_1^2 = D_3\}$ | $(2 \leftarrow 1 \times 1)$ |
| 7 | $R_3 \leftarrow R_1 \times R_3$: | $\{= Z_1^2 X_1^2 = Z_2 = D_5\}$ | $(4 \leftarrow 2 \times 2)$ |
| 8 | $R_1 \leftarrow R_1 \times R_1$: | $\{= X_1^4 = D_6\}$ | $(4 \leftarrow 2 \times 2)$ |
| 9 | $R_1 \leftarrow R_1 + R_4$: | $\{= Z_1^4 B + X_1^4 = X_2 = D_7\}$ | $(4 \leftarrow 4 + 4)$ |
| 10 | $R_2 \leftarrow R_2 \times R_2$: | $\{= Y_1^2 = D_8\}$ | $(4 \leftarrow 2 \times 2)$ |
| 11 | If $A \neq 0$ | | |
| | $R_5 \leftarrow A$ | | |
| 12 | $R_5 \leftarrow R_3 \times R_5$ | $\{= Z_2 A = D_9\}$ | $(4 \leftarrow 4 \times 0)$ |
| 13 | $R_2 \leftarrow R_5 + R_2$ | $\{= AZ_2 + Y_1^2 = D_{10}\}$ | $(4 \leftarrow 4 + 4)$ |
| 14 | $R_2 \leftarrow R_2 + R_4$: | $\{= Z_1^4 B + Z_2 A + Y_1^2 = D_{11}\}$ | $(4 \leftarrow 4 + 4)$ |
| | | or $\{= Y_1^2 + BZ_1^4 = D_{11}\}$ | $(4 \leftarrow 4 + 4)$ |
| 15 | $R_2 \leftarrow R_1 \times R_2$: | $\{= X_2(AZ_2 + Y_1^2 + BZ_1^4) = D_{12}\}$ | $(8 \leftarrow 4 \times 4)$ |
| | | or $\{= X_2(Y_1^2 + BZ_1^4) = D_{12}\}$ | $(8 \leftarrow 4 \times 4)$ |
| 16 | $R_4 \leftarrow R_3 \times R_4$: | $\{= BZ_2 Z_1^4 = D_{13}\}$ | $(8 \leftarrow 4 \times 4)$ |
| 17 | $R_2 \leftarrow R_2 + R_4$: | $\{= BZ_2 Z_1^4 + X_2(AZ_2 + Y_1^2 + BZ_1^4) = Y_2 = D_{14}\}$ | $(8 \leftarrow 8 + 8)$ |
| | | or $\{= X_2(Y_1^2 + BZ_1^4) + BZ_2 Z_1^4 = Y_2 = D_{14}\}$ | $(8 \leftarrow 8 + 8)$ |
| 18 | $X_2 \leftarrow R_1$ | | |
| 19 | $Y_2 \leftarrow R_2$ | | |
| 20 | $Z_2 \leftarrow R_3$ | | |

***Table 2.*** *Addition over Weierstrass Binary Curve.*

| **Algorithm: add**$^{\mathcal{P}}$ over Weierstrass Binary Curves [9, 18] | | | |
|---|---|---|---|
| **Input**: $(P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}, A, B)$ | | | |
| **Output**: $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2$ | | | |
| | **Operation** | **Intermediate Values** | $\mathbf{deg(Z_1)}, \mathbf{deg(Z_2)}$ |
| 1 | $R_1 \leftarrow X_1, R_2 \leftarrow Y_1$ | | |
| | $R_3 \leftarrow Z_1$ | | |
| 2 | $R_4 \leftarrow X_2, R_5 \leftarrow Y_2$ | | |
| | $R_6 \leftarrow Z_2$ | | |
| 3 | $R_7 \leftarrow R_4 \times R_3$: | $\{= Z_1 X_2 = B_0\}$ | $(1_1 1_2 \leftarrow 1_1 \times 1_2)$ |
| 4 | $R_1 \leftarrow R_6 \times R_1$: | $\{= Z_2 X_1 = B_1\}$ | $(1_1 1_2 \leftarrow 1_1 \times 1_2)$ |
| 5 | $R_3 \leftarrow R_3 \times R_6$: | $\{= Z_2 Z_1 = E\}$ | $(1_1 1_2 \leftarrow 1_1 \times 1_2)$ |
| 6 | $R_3 \leftarrow R_5 \times R_7$: | $\{Z_1^2 Y_2 = A_0\}$ | $(2_1 2_2 \leftarrow 2_1 \times 2_2)$ |
| 7 | $R_6 \leftarrow R_6 \times R_6$: | $\{Z_2^2\}$ | $(2_2 \leftarrow 1_2 \times 1_2)$ |
| 8 | $R_6 \leftarrow R_2 \times R_6$: | $\{= Z_2^2 Y_1 = A_1\}$ | $(2_1 2_2 \leftarrow 2_1 \times 2_2)$ |
| 9 | $R_2 \leftarrow R_3 + R_6$: | $\{= Z_1^2 Y_2 + Z_2^2 Y_1 = C\}$ | $(2_1 2_2 \leftarrow 2_1 2_2 + 2_1 2_2)$ |
| 10 | $R_4 \leftarrow R_1 + R_7$: | $\{= Z_1 X_2 + Z_2 X_1 = D\}$ | $(1_1 1_2 \leftarrow 1_1 1_2 + 1_1 1_2)$ |
| 11 | $R_5 \leftarrow R_4 \times R8$: | $\{(Z_1 Z_2) D = F\}$ | $(2_1 2_2 \leftarrow 1_1 1_2 \times 1_1 1_2)$ |
| 12 | $R_6 \leftarrow R_5 \times R_5$: | $\{= F^2 = Z_3\}$ | $(4_1 4_2 \leftarrow 2_1 2_2 \times 2_1 2_2)$ |
| 13 | $R_4 \leftarrow R_4 \times R_4$: | $\{= D^2\}$ | $(2_1 2_2 \leftarrow 1_1 1_2 \times 1_1 1_2)$ |
| 14 | $R_9 \leftarrow R_8 \times R_8$: | $\{= E^2\}$ | $(2_1 2_2 \leftarrow 1_1 1_2 \times 1_1 1_2)$ |
| 15 | $R_9 \leftarrow A \times R_8$: | $\{= E^2 A\}$ | $(2_1 2_2 \leftarrow 0 \times 2_1 2_2)$ |

| | Operation | Intermediate Values | $\deg(\mathbf{Z_1}), \deg(\mathbf{Z_2})$ |
|---|---|---|---|
| 16 | $R_9 \leftarrow R_5 + R_9$: | $\{= F + E^2A\}$ | $(2_12_2 \leftarrow 2_12_2 + 2_12_2)$ |
| 17 | $R_9 \leftarrow R_4 \times R_9$: | $\{= (F + E^2A)D^2 = G\}$ | $(4_14_2 \leftarrow 2_12_2 \times 2_12_2)$ |
| 18 | $R_1 \leftarrow R_2 \times R_2$: | $\{(Y_1Z_2)^2 + (Y_2Z_1)^2 = C^2\}$ | $(4_14_2 \leftarrow 2_12_2 \times 2_12_2)$ |
| 19 | $R_2 \leftarrow R_2 \times R_5$: | $\{FC = H\}$ | $(4_14_2 \leftarrow 2_12_2 \times 2_12_2)$ |
| 20 | $R_1 \leftarrow R_1 + R_2$: | $\{= H + C^2\}$ | $(4_14_2 \leftarrow 4_14_2 + 4_14_2)$ |
| 21 | $R_1 \leftarrow R_1 + R_9$: | $\{= H + G + C^2 = X_3\}$ | $(4_14_2 \leftarrow 4_14_2 + 4_14_2)$ |
| 22 | $R_5 \leftarrow R_4 \times R_7$: | $\{= D^2B_0\}$ | $(3_13_2 \leftarrow 2_12_2 \times 1_11_2)$ |
| 23 | $R_5 \leftarrow R_5 \times R_8$: | $\{= D^2EB_0\}$ | $(4_14_2 \leftarrow 3_13_2 \times 1_11_2)$ |
| 24 | $R_5 \leftarrow R_5 + R_1$: | $\{= B_0D^2E + X_3 = I\}$ | $(4_14_2 \leftarrow 4_14_2 + 4_14_2)$ |
| 25 | $R_8 \leftarrow R_4 + R_3$: | $\{= D^2A_0\}$ | $(4_14_2 \leftarrow 2_12_2 \times 2_12_2)$ |
| 26 | $R_8 \leftarrow R_8 + R_2$: | $\{= X_3 + A_0D^2 = J\}$ | $(4_14_2 \leftarrow 4_14_2 + 4_14_2)$ |
| 27 | $R_8 \leftarrow R_6 \times R_8$: | $\{= JZ_3\}$ | $(8_18_2 \leftarrow 4_14_2 \times 4_14_2)$ |
| 28 | $R_2 \leftarrow R_2 \times R_5$: | $\{= IH\}$ | $(8_18_2 \leftarrow 4_14_2 \times 4_14_2)$ |
| 29 | $R_2 \leftarrow R_2 + R_8$: | $\{= Z_3J + HI = Y_3\}$ | $(8_18_2 \leftarrow 8_18_2 + 8_18_2)$ |

### *2.2.2. Edwards Binary Curves in Projective Coordinates*

*Projective Doubling:* Let $P_1 = (x_1, y_1)$ be a point on a binary Edwards curve $E$ with the coefficients $d_1, d_2$. In projective coordinates, $P_1 = (X_1, Y_1, Z_1)$ where $X_1 = x_1Z_1, Y_1 = Y_1Z_1$, $P_3 = (X_3, Y_3, Z_3) = 2P_1$ is computed as follows:

***Table 3.*** *Doubling over Edwards Binary Curve.*

| **Algorithm:dbl**$^{\mathcal{P}}$ over Edwards Binary Curves [16] | | |
|---|---|---|
| **Input**: $(P_1 \neq \mathcal{O})$ | | |
| **Output**: $P_3 = (X_3, Y_3, Z_3) = 2P_1$ | | |
| | **Operation** | **Operations on** $\deg(\mathbf{Z_1})$ |
| 1 | $A = X_1^2$ | $(2 \leftarrow 1 \times 1)$ |
| 2 | $B = A^2$ | $(4 \leftarrow 2 \times 2)$ |
| 3 | $C = Y_1^2$ | $(2 \leftarrow 1 \times 1)$ |
| 4 | $D = C^2$ | $(4 \leftarrow 2 \times 2)$ |
| 5 | $AE = Z_1^2$ | $(2 \leftarrow 1 \times 1)$ |
| 6 | $T_0 = E^2$ | $(4 \leftarrow 2 \times 2)$ |
| 7 | $F = d_1T_0$ | $(4 \leftarrow 0 \times 4)$ |
| 8 | $T_1 = B + D$ | $(4 \leftarrow 4 + 4)$ |
| 9 | $G = \frac{d_2}{d_1}T_0$ | $(4 \leftarrow 0 \times 4)$ |
| 10 | $H = A \times E$ | $(4 \leftarrow 2 \times 2)$ |
| 11 | $I = C \times E$ | $(4 \leftarrow 2 \times 2)$ |
| 12 | $J = H + I$ | $(4 \leftarrow 4 + 4)$ |
| 13 | $T_2 = d_2J$ | $(4 \leftarrow 0 \times 4)$ |
| 14 | $K = G + T_2$ | $(4 \leftarrow 4 + 4)$ |
| 15 | $T_3 = F + J$ | $(4 \leftarrow 4 + 4)$ |
| 16 | $Z_3 = T_3 + G$ | $(4 \leftarrow 4 + 4)$ |
| 17 | $T_4 = K + H$ | $(4 \leftarrow 4 + 4)$ |
| 18 | $X_3 = T_4 + D$ | $(4 \leftarrow 4 + 4)$ |
| 19 | $T_5 = K + I$ | $(4 \leftarrow 4 + 4)$ |
| 20 | $Y_3 = T_5 + B$ | $(4 \leftarrow 4 + 4)$ |

*Projective Addition:* Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ two points on a binary Edwards curve $E$ with the coefficients $d_1, d_2$. In projective coordinates, $P_1 = (X_1, Y_1, Z_1)$ where $X_1 = x_1Z_1, Y_1 = Y_1Z_1$, and $P_2 = (X_2, Y_2, Z_2)$ where $X_2 = x_2Z_2, Y_2 = Y_2Z_2$ $P_3 = (X_3, Y_3, Z_3) = P_1 + p_2$ is computed as follows:

***Table 4.*** *Addition over Edwards Binary Curve.*

| **Algorithm: add**$^{\mathcal{P}}$ over Edwards Binary Curves [16] | | |
|---|---|---|
| **Input**: $(P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}, A, B)$ | | |
| **Output**: $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2$ | | |
| | **Operation** | **Operation on** $\deg(\mathbf{Z_1}), \deg(\mathbf{Z_2})$ |
| 1 | $W_1 = X_1 + Y_1$: | $(1_1 \leftarrow 1_1 + 1_1)$ |

| | Operation | Operation on $\mathbf{deg(Z_1)}, \mathbf{deg(Z_2)}$ |
|---|---|---|
| 2 | $W_2 = X_2 + Y_2$: | $(1_2 \leftarrow 1_2 + 1_2)$ |
| 3 | $T_0 = X_1 + Z_1$: | $(1_1 \leftarrow 1_1 + 1_1)$ |
| 4 | $A = X_1 \times T_0$: | $(2_1 \leftarrow 1_1 \times 1_1)$ |
| 5 | $T_1 = Y_1 + Z_1$: | $(1_1 \leftarrow 1_1 + 1_1)$ |
| 6 | $B = Y_1 \times T_1$: | $(2_1 \leftarrow 1_1 \times 1_1)$ |
| 7 | $C = Z_1 \times Z_2$: | $(1_1 1_2 \leftarrow 1_1 \times 1_2)$ |
| 8 | $D = W_2 \times Z_2$: | $(2_2 \leftarrow 1_2 \times 1_2)$ |
| 9 | $T_2 = C \times C$: | $(2_1 2_2 \leftarrow 1_1 1_2 \times 1_1 1_2)$ |
| 10 | $E = d_1 \times T_2$: | $(2_1 2_2 \leftarrow 0 \times 2_1 2_2)$ |
| 11 | $T_3 = d_2 \times W_2$: | $(1_2 \leftarrow 0 \times 1_2)$ |
| 12 | $T_4 = d_1 \times Z_2$: | $(1_2 \leftarrow 0 \times 1_2)$ |
| 13 | $T_5 = T_4 + T_3$: | $(1_2 \leftarrow 12 + 1_2)$ |
| 14 | $T_6 = W_1 \times C$: | $(2_1 1_2 \leftarrow 1_1 \times 1_1 1_2)$ |
| 15 | $H = T_5 \times T_6$: | $(2_1 2_2 \leftarrow 1_2 \times 2_1 1_2)$ |
| 16 | $T_7 = Z_1 \times C$: | $(2_1 1_2 \leftarrow 1_1 \times 1_1 1_2)$ |
| 18 | $I = d_1 \times T_7$: | $(2_1 1_2 \leftarrow 0 \times 2_1 1_2)$ |
| 19 | $T_8 = A \times D$: | $(2_1 2_2 \leftarrow 2_1 \times 2_2)$ |
| 20 | $U = E + T_8$: | $(2_1 1_2 \leftarrow 2_1 1_2 + 2_1 1_2)$ |
| 21 | $T_9 = B \times D$: | $(2_1 2_2 \leftarrow 2_1 \times 2_2)$ |
| 22 | $V = E + T_9$: | $(2_1 1_2 \leftarrow 2_1 1_2 + 2_1 1_2)$ |
| 23 | $S = U \times V$: | $(4_1 4_2 \leftarrow 2_1 1_2 \times 2_1 1_2)$ |
| 24 | $T_{10} = Y_2 + Z_2$: | $(1_2 \leftarrow 1_2 + 1_2)$ |
| 25 | $T_{11} = A \times T_{10}$: | $(2_1 1_2 \leftarrow 2_1 \times 1_2)$ |
| 26 | $T_{12} = I + T_{11}$: | $(2_1 1_2 \leftarrow 2_1 1_2 + 2_1 1_2)$ |
| 27 | $T_{13} = X_2 \times T_{12}$: | $(2_1 2_2 \leftarrow 1_2 \times 2_1 1_2)$ |
| 28 | $T_{14} = H + T_{13}$: | $(2_1 2_2 \leftarrow 2_1 2_2 + 2_1 2_2)$ |
| 29 | $T_{15} = V \times Z_1$: | $(3_1 2_2 \leftarrow 2_1 1_2 \times 1_1)$ |
| 30 | $T_{16} = T_{14} \times T_{15}$: | $(5_1 4_2 \leftarrow 2_1 1_2 \times 3_1 2_2)$ |
| 31 | $T_{17} = S \times Y_1$: | $(5_1 4_2 \leftarrow 4_1 4_2 \times 1_1)$ |
| 32 | $X_3 = T_{16} + T_{17}$: | $(5_1 4_2 \leftarrow 5_1 4_2 + 5_1 4_2)$ |
| 33 | $T_{18} = X_2 + Z_2$: | $(1_2 \leftarrow 1_2 + 1_2)$ |
| 34 | $T_{19} = B \times T_{18}$: | $(2_1 1_2 \leftarrow 2_1 \times 1_2)$ |
| 35 | $T_{20} = I + T_{19}$: | $(2_1 1_2 \leftarrow 2_1 1_2 + 2_1 1_2)$ |
| 36 | $T_{21} = Y_2 \times T_{20}$: | $(2_1 1_2 \leftarrow 1_2 \times 2_1 1_2)$ |
| 37 | $T_{22} = H + T_{21}$: | $(2_1 2_2 \leftarrow 2_1 2_2 + 2_1 2_2)$ |
| 38 | $T_{23} = U \times Z_1$: | $(3_1 2_2 \leftarrow 2_1 1_2 \times 1_1)$ |
| 39 | $T_{24} = T_{22} \times T_{23}$: | $(5_1 4_2 \leftarrow 2_1 1_2 \times 3_1 2_2)$ |
| 40 | $T_{25} = S \times X_1$: | $(5_1 4_2 \leftarrow 4_1 4_2 \times 1_1)$ |
| 41 | $Y_3 = T_{24} + T_{25}$: | $(5_1 4_2 \leftarrow 5_1 4_2 + 5_1 4_2)$ |
| 42 | $Z_3 = S \times Z_1$: | $(5_1 4_2 \leftarrow 4_1 4_2 \times 1_1)$ |

### *2.2.3. Hessian Binary Curves in Projectives Coordinates*

*Projective Doubling*: Let $P_1 = (x_1, y_1)$ be a point on a binary Hessian curve $E$ with the coefficients $d$. In projective coordinates, $P_1 = (X_1, Y_1, Z_1)$ where $X_1 = x_1 Z_1, Y_1 = Y_1 Z_1$, $P_3 = (X_3, Y_3, Z_3) = 2P_1$ is computed as follows:

***Table 5.*** *Doubling over Hessian Binary Curve.*

| **Algorithm:dbl**$^{\mathcal{P}}$ over Hessian Binary Curves<br>**Input**: $(P_1 \neq \mathcal{O})$<br>**Output**: $P_3 = 2P_1$ | | | |
|---|---|---|---|
| | **Operation** | **Values Computed** | $\mathbf{deg(Z_1)}$ |
| 1 | $T_1 \leftarrow Z_1, T_2 \leftarrow X_1,$<br>$T_3 \leftarrow Y_1$ | | |
| 2 | $T_4 \leftarrow Y_1$ | | |

| | **Operation** | **Values Computed** | $\mathbf{deg(Z_1)}$ |
|---|---|---|---|
| 3 | $T_5 \leftarrow Z_1$ | | |
| 4 | $T_6 \leftarrow X_1$ | | |
| 5 | $T_7 \leftarrow T_1 \times T_6$: | $\{= X_1Z_1\}$ | $(2 \leftarrow 1 \times 1)$ |
| 6 | $T_1 \leftarrow T_1 \times T_5$: | $\{= Z_1^2\}$ | $(2 \leftarrow 1 \times 1)$ |
| 7 | $T_5 \leftarrow T_3 \times T_5$: | $\{= Y_1Z_1\}$ | $(2 \leftarrow 1 \times 1)$ |
| 8 | $T_3 \leftarrow T_3 \times T_4$: | $\{= Y_1^2\}$ | $(2 \leftarrow 1 \times 1)$ |
| 9 | $T_4 \leftarrow T_2 \times T_4$: | $\{= X_1Y_1\}$ | $(2 \leftarrow 1 \times 1)$ |
| 10 | $T_2 \leftarrow T_2 \times T_6$: | $\{= X_1^2\}$ | $(2 \leftarrow 1 \times 1)$ |
| 11 | $T_6 \leftarrow T_2 \times T_7$: | $\{= X_1^3Z_1\}$ | $(4 \leftarrow 2 \times 2)$ |
| 12 | $T_2 \leftarrow T_2 \times T_4$: | $\{= X_1^3Y_1\}$ | $(4 \leftarrow 2 \times 2)$ |
| 13 | $T_4 \leftarrow T_3 \times T_4$: | $\{= X_1^2Y_1^2\}$ | $(4 \leftarrow 2 \times 2)$ |
| 14 | $T_3 \leftarrow T_3 \times T_5$: | $\{= Y_1^3Z_1\}$ | $(4 \leftarrow 2 \times 2)$ |
| 15 | $T_5 \leftarrow T_1 \times T_5$: | $\{= Z_1^3Y_1\}$ | $(4 \leftarrow 2 \times 2)$ |
| 16 | $T_1 \leftarrow T_1 \times T_7$: | $\{= X_1Z_1^3\}$ | $(4 \leftarrow 2 \times 2)$ |
| 17 | $T_1 \leftarrow T_1 - T_4$: | $\{= X_1Z_1^3 - X_1Y_1^3\}$ | $(4 \leftarrow 4 - 4)$ |
| 18 | $T_2 \leftarrow T_2 - T_5$: | $\{= X_1^3Y_1 - Y_1Z_1^3\}$ | $(4 \leftarrow 4 - 4)$ |
| 19 | $T_3 \leftarrow T_3 - T_6$: | $\{= Y_1^3Z_1 - X_1^3Z_1\}$ | $(4 \leftarrow 4 - 4)$ |
| 20 | $X_3 \leftarrow T_2$ | | |
| 21 | $Y_3 \leftarrow T_1$ | | |
| 22 | $Z_3 \leftarrow T_3$ | | |

*Projective Addition:* Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ points on a binary Hessian curve $E$ with the coefficients $d$. In projective coordinates, $P_1 = (X_1, Y_1, Z_1)$ where $X_1 = x_1Z_1, Y_1 = Y_1Z_1$, and $P_2 = (X_2, Y_2, Z_2)$ where $X_2 = x_2Z_2, Y_2 = Y_2Z_2$ $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2$ is computed as follows:

***Table 6.*** *Addition over Hessian Binary Curve.*

| **Algorithm: add**$^{\mathcal{P}}$ over Hessian Binary Curve<br>**Input**: $(P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}, A, B)$<br>**Output**: $P_3 = P_1 + P_2$ | | | |
|---|---|---|---|
| | **Operation** | **Intermediate Values** | $\mathbf{deg(Z_1)}, \mathbf{deg(Z_2)}$ |
| 1 | $T_1 \leftarrow X1, T_2 \leftarrow Y_1, T_3 \leftarrow Z_1$ | | |
| 2 | $T_4 \leftarrow X_2, T_5 \leftarrow Y_2, T_6 \leftarrow Z_2$ | | |
| 3 | $T_7 \leftarrow T_1 \times T_6$: | $\{= X_1Z_2\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 4 | $T_1 \leftarrow T_1 \times T_5$: | $\{= X_1Y_2\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 5 | $T_5 \leftarrow T_3 \times T_5$: | $\{= Y_2Z_1\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 6 | $T_3 \leftarrow T_3 \times T_4$: | $\{= X_2Z_1\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 7 | $T_4 \leftarrow T_2 \times T_4$: | $\{= X_2Y_1\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 8 | $T_2 \leftarrow T_2 \times T_6$: | $\{= Y_1Z_2\}$ | $(1_11_2 \leftarrow 1_1 \times 1_2)$ |
| 9 | $T_6 \leftarrow T_2 \times T_7$: | $\{= X_1Y_1Z_2^2\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 10 | $T_2 \leftarrow T_2 \times T_4$: | $\{= X_2Y_1^2Z_2\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 11 | $T_4 \leftarrow T_3 \times T_4$: | $\{= X_2^2Y_1Z_1\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 12 | $T_3 \leftarrow T_3 \times T_5$: | $\{= X_2Y_2Z_1^2\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 13 | $T_5 \leftarrow T_1 \times T_5$: | $\{= X_1Y_2^2Z_1\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 13 | $T_1 \leftarrow T_1 \times T_7$: | $\{= X_1^2Y_2Z_2\}$ | $(2_12_2 \leftarrow 1_11_2 \times 1_11_2)$ |
| 14 | $T_1 \leftarrow T_1 - T_4$: | $\{= X_1^2Y_2Z_2 - X_2^2Y_1Z_1\}$ | $(2_12_2 \leftarrow 2_12_2 - 2_12_2)$ |
| 15 | $T_2 \leftarrow T_2 - T_4$: | $\{= X_2Y_1^2Z_2 - X_1Y_2^2Z_1\}$ | $(2_12_2 \leftarrow 2_12_2 - 2_12_2)$ |
| 16 | $T_3 \leftarrow T_3 - T_6$: | $\{= X_2Y_2Z_1^2 - X_1Y_1Z_2^2\}$ | $(2_12_2 \leftarrow 2_12_2 - 2_12_2)$ |
| 17 | $X_3 \leftarrow T_2$ | | |
| 18 | $Y_3 \leftarrow T_1$ | | |
| 19 | $Z_3 \leftarrow T_3$ | | |

It is very important to recall quite explicitly all the addition formulas that we made above because for the SVA attack these explicit formulas are supposed to be known in advance and the attack is essentially based on these formulas. Let us now recall the principle of this attack

### 2.3. Review of the Same Values Analysis (SVA) Attack on Elliptic Curve Defined over Fields of Odd Characteristic

Before presenting the work we have done on binary curves, it is important to recall what has been done on the curves defined on odd characteristic fields

The main idea of **SVA** is to cause an internal collision when implementing scalar multiplication. This collision will be visible if we have obtained the same intermediate values when doubling or squaring the values on the field, because this will mean that we have performed the same operation several times with the same inputs. if

$$E : y^2 = x^3 + ax + b$$

is defined over a finite field $\mathbb{F}_p$ with prime $p > 3$, $P = (x, y)$ is a collision same values point if and one of the following conditions is satisfying:

$$(\mathbf{WPDC2}) : x = 1, \quad (\mathbf{WPDC3}) : x^2 = y, \quad (\mathbf{WPDC15}) : 2y = 3x^2.$$

Similarly, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are collision same values point for addition if they satisfy the condition

$$(\mathbf{WPAC9}) : y_2 - y_1 = x_2 - x_1.$$

Let $k = (k_{n-1}....k_1k_0)_2$ be the secret key. To determine bit $k_i$ , we use the bits already found and a point $P$ which satisfies one of the collision conditions.We choose a base point as $P_0 = ((k_{n-1}....k_{i+1})_2)^{-1}\text{Mod}[\#E(\mathbb{K})]P$, where $\#E(\mathbb{K})$ is the cardinality of the elliptic curve. When scalar multiplication is implemented with the base point $P_0$ and the secret key $k$, the collision point $P$ will be double and this collision will be visible if the bit $k_i = 0$, else $k_i = 1$. The attacker can recursively recover all bits of $k$.

## 3. Same Values Analysis over Binary Elliptic Curves

We now turn to the attack on binary curves. We will proceed as follows: we will first search for the points with zero.

### 3.1. Special Points of Same Values During Doubling

#### 3.1.1. Special Point for Doubling on Weierstrass Curve

This case is the result of our work [19] published at the International Cryptography Conference for Africa in 2024, abbreviated as Africacrypt 2024. Here, we provide a detailed presentation of our proofs, making them clearer and easier to understand.

Let $E : y^2 + xy = x^3 + Ax + B,$ be an Weierstrass curve, where $A, B \in \mathbb{K}$.

Let $P_1 = (x_1, y_1)$ be a point on the elliptic curve $E$, in projective coordinates $P_1 = (Z_1x_1 : Z_1^2y_1 : Z_1)$ for some $Z \in \mathbb{K}$. Let $P_3 = (X_3 : Y_3 : Z_3) = 2P_1$. Theorem 3.1 summarizes all conditions that a point will verify to be same value point for doubling on elliptic curve over a binary field. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for doubling on binary Weierstrass curves by *WBDC*.

*Theorem* 3.1. [19] Let E be an elliptic curve defined by the equation $y^2+xy = x^3+Ax^2+B$ over a binary field $\mathbb{K}$, where $m$ is a positive integer. The point $P_1 = (x_1, y_1) \in E$ is a same values point relative to the algorithm $dbl^{\mathcal{P}}(P_1)$ if and only if one of the following conditions given below is satisfied:

| | | | |
|---|---|---|---|
| $c = 1$ | $(WBDC1)$ | $x_1 = 1$ | $(WBDC2)$ |
| $x_1^2 = c$ | $(WBDC3)$ | $x_1^2 = B$ | $(WBDC4)$ |
| $x_1^4 = B$ | $(WBDC5)$ | $x_1 = 0$ | $(WBDC6)$ |
| $y_1^2 + B = 0$ | $(WBDC7)$ | $Ax_1^2 + B = 0$ | $(WBDC8)$ |
| $y_1^2 + Ax_1^2 = B$ | $(WBDC9)$ | $y_1 = 0$ or $y_1^2 + Ax_1^2 = 0$ | $(WBDC10)$ |
| $x_1^4 + x_1^2 + B = 0$ | $(WBDC11)$ | $x_1 = y_1$ | $(WBDC12)$ |
| $A = 1$ | $(WBDC13)$ | $(A + 1)x_1^2 + y_1^2 = 0$ | $(WBDC14)$ |
| $B = 0$ | $(WBDC15)$ | $(A+1)x_1^2 + y_1^2 + B = 0$ or $x_1^2 + y_1^2 + B = 0$ | $(WBDC16)$ |
| $x_1^2 = y_1$ | $(WBDC17)$ | $x_1^2 = A$ | $(WBDC18)$ |
| $x_1^4 + Ax_1^2 + y_1^2 = 0$ | $(WBDC19)$ | $x_1^4 + y_1^2 + B = 0$ or $x_1^4 + Ax_1^2 + y_1^2 + B = 0$ | $(WBDC20)$ |
| $x_1^4 + y_1^2 + B = 0$ | $(WBDC21)$ | $x_1^4 + Ax_1^2 + B = 0$ | $(WBDC22)$ |
| $A = 0$ | $(WBDC23)$ | $Ax_1^4 + (1 + A)B = 0$ | $(WBDC24)$ |
| $(A + 1)x_1^2 + y_1^2 + B = 0$ or $x_1^2 + y_1^2 + B = 0$ | | | $(WBDC25)$ |
| $Bx_1^4 + x_1^4y_1^2 + By_1^2 + Bx_1^2 + B^2 = 0$ or $Ax_1^6 + x_1^4y_1^2 + Bx_1^4 + B(A + 1)x_1^2 + By_1^2 + B^2 = 0$ | | | $(WBDC26)$ |

*Proof.* Let $P = P_1 = (x_1, y_1)$ be a point on the elliptic curve

$$E : y^2 + xy = x^3 + Ax^2 + B$$

defined over the binary field $\mathbb{K}$. In projective coordinates, we have:

$$x_1 = \frac{X_1}{Z_1},\ y_1 = \frac{Y_1}{Z_1^2},\ \text{so}\ P_1 = (X_1 : Y_1 : Z_1) = (Z_1 x_1 : Z_1^2 y_1 : Z_1).$$

We are interested in identifying equalities between intermediate expressions involving the same degree of $Z_1$, and also in detecting when any of these expressions evaluate to zero. Let $S_i$ denote the set of intermediate values involving terms with degree $i$ in $Z_1$. When analyzing the point doubling algorithm $dbl^{\mathcal{P}}(P_1)$ over binary elliptic curves in projective coordinates, the following sets are obtained:

1. $S_2 = \{D_1, D_2, D_3\}$.
2. $S_4 = \{D_4, D_5, D_6, D_7, D_8, D_9, D_{10}, D_{11}\}$.
3. $S_8 = \{D_{12}, D_{13}, D_{14}\}$.

Equalities can only occur between expressions within the same set $S_i$. Comparing each pair of expressions within these sets, we obtain the following equalities:

1. *Within $S_2$:*
   $D_1 = D_2 \Rightarrow$ (WBDC 1),
   $D_1 = D_3 \Rightarrow$ (WBDC 2),
   $D_2 = D_3 \Rightarrow$ (WBDC 3).
2. *Within $S_4$:*
   $D_4 = D_5 \Rightarrow$ (WBDC 4),
   $D_4 = D_6 \Rightarrow$ (WBDC 5),
   $D_4 = D_7 \Rightarrow$ (WBDC 6),
   $D_4 = D_8 \Rightarrow$ (WBDC 7),
   $D_4 = D_9 \Rightarrow$ (WBDC 8),
   $D_4 = D_{10} \Rightarrow$ (WBDC 9),
   $D_4 = D_{11} \Rightarrow$ (WBDC 10),
   $D_5 = D_6 \Rightarrow$ (WBDC 2) and WBDC 6)
   $D_5 = D_7 \Rightarrow$ (WBDC 11),
   $D_5 = D_8 \Rightarrow$ (WBDC 12),
   $D_5 = D_9 \Rightarrow$ (WBDC 6) and WBDC 13)
   $D_5 = D_{10} \Rightarrow$ (WBDC 14),
   $D_5 = D_{11} \Rightarrow$ (WBDC 16),
   $D_6 = D_7 \Rightarrow$ (WBDC 15),
   $D_6 = D_8 \Rightarrow$ (WBDC 6) and WBDC 18)
   $D_6 = D_9 \Rightarrow$ (WBDC 6) and WBDC 18)
   $D_6 = D_{10} \Rightarrow$ (WBDC 19),
   $D_6 = D_{11} \Rightarrow$ (WBDC 20) and WBDC 21)
   $D_7 = D_8 \Rightarrow$ (WBDC 21),
   $D_7 = D_9 \Rightarrow$ (WBDC 22),
   $D_7 = D_{10} \Rightarrow$ (WBDC 20),
   $D_7 = D_{11} \Rightarrow$ (WBDC 17) and WBDC 19)
   $D_8 = D_9 \Rightarrow$ (WBDC 10) ( first part)
   $D_8 = D_{10} \Rightarrow$ (WBDC 6) and WBDC 23)
   $D_8 = D_{11} \Rightarrow$ (WBDC 8) and WBDC 15)
   $D_9 = D_{10} \Rightarrow$ (WBDC 10) (second part)
   $D_9 = D_{11} \Rightarrow$ (WBDC 7) and WBDC 9)
   $D_{10} = D_{11} \Rightarrow$ (WBDC 15) and WBDC 8).
3. *Within $S_8$:*
   $D_{12} = D_{13} \Rightarrow$ (WBDC 26),
   $D_{12} = D_{14} \Rightarrow$ (WBDC 6) , WBDC 15) and WBDC 24)
   $D_{13} = D_{14} \Rightarrow$ (WBDC 25).

We are now interested on special point on same values during doubling in the case of Edwards binary curve.

#### *3.1.2. Special Point for Doubling on Edwards Curve*

We recall that an elliptic curve over binary fields is defined as follows:

$$E : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$$

, where $d_1, d_2 \in \mathbb{K}$.

Let $P_1 = (x_1, y_1)$ be a point on the elliptic curve $E$, in projective coordinates $P_1 = (Z_1x_1 : Z_1y_1 : Z_1)$ for some $Z \in \mathbb{K}$. Let $P_3 = (X_3 : Y_3 : Z_3) = 2P_1$.

Theorem 3.2 summarizes all conditions that a point will verify to be same-values point for doubling on elliptic curve over Edwards binary fields. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for doubling on binary Edwards curves by *EBDC*.

*Theorem* 3.2. Let E be an Edwards binary elliptic curve over $\mathbb{K}$, defined by the equation $E : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$. The point $P = (x, y) \in E$ is a same-value point relative to the algorithm $dbl^{\mathcal{P}}$ if and only if one of the following conditions given below are satisfied:

| | | | |
|---|---|---|---|
| $x = y$ | $(EBDC1)$ | $x = 1$ | $(EBDC2)$ |
| $x^4 = d_1$ | $(EBDC3)$ | $y = 0$ | $(EBDC4)$ |
| $x^4 = \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC5)$ | $x = 0$ | $(EBDC6)$ |
| $x^2 = y$ | $(EBDC7)$ | $x^4 = x^2 + y^2$ | $(EBDC8)$ |
| $x^4 = d_2(x^2 + y^2)$ | $(EBDC9)$ | $x^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC10)$ |
| $x^4 = d_1 + x^2 + y^2$ | $(EBDC11)$ | $x^4 = d_1 + x^2 + y^2 + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC12)$ |
| $x^4 = x^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC13)$ | $x^4 = y^4 + x^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC14)$ |
| $x^4 = y^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC15)$ | $y^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC16)$ |
| $y = 1$ | $(EBDC17)$ | $y^4 = d_1$ | $(EBDC18)$ |
| $y^4 = \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC19)$ | $y^2 = x$ | $(EBDC20)$ |
| $y^4 = x^2 + y^2$ | $(EBDC21)$ | $y^4 = d_2(x^2 + y^2)$ | $(EBDC22)$ |

| | | | |
|---|---|---|---|
| $y^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC23)$ | $y^4 = d_1 + x^2 + y^2$ | $(EBDC24)$ |
| $y^4 = d_1 + x^2 + y^2 + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC25)$ | $y^4 = x^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC26)$ |
| $x^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC27)$ | $y^4 = y^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC28)$ |
| $y^4 = y^2 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^4)$ | $(EBDC29)$ | | |
| $d_1 = 1$ | $(EBDC30)$ | $x^4 + y^4 = 1$ | $(EBDC31)$ |
| $x^2 + y^2 = 1$ | $(EBDC32)$ | $d_2(x^2 + y^2) = 1$ | $(EBDC33)$ |
| $d_1 = d_2(x^4 + y^4)$ | $(EBDC34)$ | $1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC35)$ |
| $d_1 + x^2 + y^2 = 1$ | $(EBDC36)$ | $d_1 + x^2 + y^2 + \frac{d_2}{d_1}(x^4 + y^4) = 1$ | $(EBDC37)$ |
| $1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2$ | $(EBDC38)$ | $1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2 + y^4$ | $(EBDC39)$ |
| $1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2$ | $(EBDC40)$ | $1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2 + x^4$ | $(EBDC41)$ |
| $d_1 = x^4 + y^4$ | $(EBDC42)$ | $d_1 = \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC43)$ |
| $d_1 = x^2$ | $(EBDC44)$ | $d_1 = y^2$ | $(EBDC45)$ |
| $d_1 = x^2 + y^2$ | $(EBDC46)$ | $d_1 = d_2(x^2 + y^2)$ | $(EBDC47)$ |
| $d_1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC48)$ | $x^2 + y^2 + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC49)$ |
| $d_1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2$ | $(EBDC50)$ | $d_1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2 + y^4$ | $(EBDC51)$ |
| $d_1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2$ | $(EBDC52)$ | $d_1 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2 + x^4$ | $(EBDC53)$ |
| $d_1 = d_2$ | $(EBDC54)$ | $x^4 + y^4 = x^2$ | $(EBDC55)$ |
| $x^4 + y^4 = y^2$ | $(EBDC56)$ | $x^4 + y^4 = x^2 + y^2$ | $(EBDC57)$ |
| $x^4 + y^4 = d_2(x^2 + y^2)$ | $(EBDC58)$ | $x^4 + y^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC59)$ |
| $x^4 + y^4 = x^2 + y^2 + d_1$ | $(EBDC60)$ | $x^4 + y^4 = x^2 + y^2 + d_1 + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC61)$ |
| $x^4 + y^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2$ | $(EBDC62)$ | $x^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2$ | $(EBDC63)$ |
| $x^4 + y^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2$ | $(EBDC64)$ | $y^4 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2$ | $(EBDC65)$ |
| $\frac{d_2}{d_1}(x^4 + y^4) = x^2$ | $(EBDC66)$ | $\frac{d_2}{d_1}(x^4 + y^4) = y^2$ | $(EBDC67)$ |
| $\frac{d_2}{d_1}(x^4 + y^4) = x^2 + y^2$ | $(EBDC68)$ | $\frac{d_2}{d_1}(x^4 + y^4) = d_2(x^2 + y^2)$ | $(EBDC69)$ |
| $\frac{d_2}{d_1}(x^4 + y^4) = x^2 + y^2 + d_1$ | $(EBDC70)$ | $d_2(x^2 + y^2) + x^2 = 0$ | $(EBDC71)$ |
| $d_2(x^2 + y^2) + x^2 + y^4 = 0$ | $(EBDC72)$ | $d_2(x^2 + y^2) + y^2 = 0$ | $(EBDC73)$ |
| $d_2(x^2 + y^2) + y^2 + x^4 = 0$ | $(EBDC74)$ | $x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC75)$ |
| $d_1 + y^2 + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC76)$ | $y^4 + d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC77)$ |
| $x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^2$ | $(EBDC78)$ | $x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + x^4) + y^2 + x^4$ | $(EBDC79)$ |
| $y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC80)$ | $d_1 + x^2 + \frac{d_2}{d_1}(x^4 + y^4) = 0$ | $(EBDC81)$ |
| $y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^2 + y^4$ | $(EBDC82)$ | $d_2 = 0$ | $(EBDC83)$ |
| $x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^4$ | $(EBDC84)$ | $y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^4$ | $(EBDC85)$ |
| $d_1 + y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC86)$ | $d_1 + y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + y^4$ | $(EBDC87)$ |
| $d_1 + x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC88)$ | $d_1 + x^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4) + x^4$ | $(EBDC89)$ |
| $d_1 + x^2 + y^2 = d_2(x^2 + y^2)$ | $(EBDC90)$ | $d_1 + x^2 + y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC91)$ |
| $x^2 + y^4 = \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC92)$ | $y^4 + x^2 = \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC93)$ |
| $d_1 + x^2 + y^2 = d_2(x^2 + y^2) + \frac{d_2}{d_1}(x^4 + y^4)$ | $(EBDC94)$ | $d_1 + y^2 = d_2(x^2 + y^2)$ | $(EBDC95)$ |
| $d_1 + y^2 = d_2(x^2 + y^2) + y^4$ | $(EBDC96)$ | $d_1 + x^2 = d_2(x^2 + y^2)$ | $(EBDC97)$ |
| $d_1 + x^2 = d_2(x^2 + y^2) + x^4$ | $(ED98)$ | | |

*Proof.* Let $P_1 = (x_1, y_1)$ be a point on the elliptic curve

$$E : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$$

defined over a binary $\mathbb{K}$, where $m$ is a positive integer. In projective coordinates, we have $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1$, so the point $P_1$ is represented as $P_1 = (X_1 : Y_1 : Z_1) = (Z_1x_1 : Z_1y_1 : Z_1)$.

We aim to identify equalities between expressions involving the same degree of $Z_1$, as well as zero-value terms among all expressions. Let $S_i$ denote the set of expressions involving $Z_1$ raised to the power $i$. When analyzing the point doubling algorithm $dbl^{\mathcal{P}}(P_1)$ for elliptic curves over binary Edwards fields in projective coordinates, we obtain:

1. $S_2 = \{A, C, E\}$
2. $S_4 =$

$$\{B, D, T_0, F, T_1, G, H, I, J, T_2, K, T_3, Z_3, T_4, X_3, T_5, Y_3\}$$

Equalities can only occur between expressions within the same subset. To identify them, we compare terms pairwise within each set.

The condition $(EBDC1)$ is defined by the following equalities: $B = D$, $A = C$, $I = H$, $F = T_3$, $G = K$, $J = T_2$, $T_2 = K$, $T_3 = Z_3$.

$(EBDC2)$ is given by: $B = T_0$, $A = E$, $B = H$, $T_0 = H$.
$(EBDC3)$: $B = F$.
$(EBDC4)$: $B = T_1$, $D = I$, $H = J$, $K = T_5$.
$(EBDC5)$: $B = G$.
$(EBDC6)$: $B = H$, $D = T_1$, $I = J$, $K = T_4$.
$(EBDC7)$: $B = I$, $K = Y_3$.
$(EBDC8)$: $B = J$.
$(EBDC9)$: $B = T_2$.

$(EBDC10)$: $B = K$.
$(EBDC11)$: $B = T_3$.
$(EBDC12)$: $B = Z_3$.
$(EBDC13)$: $B = T_4$.
$(EBDC14)$: $B = X_3$.
$(EBDC15)$: $B = T_5$.
$(EBDC16)$: $B = Y_3$.
$(EBDC17)$: $C = E$, $D = T_0$, $D = I$, $T_0 = I$.
$(EBDC18)$: $D = F$.
$(EBDC19)$: $D = G$.
$(EBDC20)$: $D = H$, $K = X_3$.
$(EBDC21)$: $D = J$.
$(EBDC22)$: $D = T_2$.
$(EBDC23)$: $D = K$.
$(EBDC24)$: $D = T_3$.
$(EBDC25)$: $D = Z_3$.
$(EBDC26)$: $D = T_4$.
$(EBDC27)$: $D = X_3$.
$(EBDC28)$: $D = T_5$.
$(EBDC29)$: $D = Y_3$.
$(EBDC30)$: $T_0 = F$.
$(EBDC31)$: $T_0 = T_1$, $T_1 = G$.
$(EBDC32)$: $T_0 = J$.
$(EBDC33)$: $T_0 = T_2$.
$(EBDC34)$: $T_0 = G$.
$(EBDC35)$: $T_0 = K$.
$(EBDC36)$: $T_0 = T_3$.
$(EBDC37)$: $T_0 = Z_3$.
$(EBDC38)$: $T_0 = T_4$.
$(EBDC39)$: $T_0 = X_3$.
$(EBDC40)$: $T_0 = T_5$.
$(EBDC41)$: $T_0 = Y_3$.
$(EBDC42)$: $F = T_1$.
$(EBDC43)$: $F = G$.
$(EBDC44)$: $F = H$, $I = T_3$, $J = Z_3$.
$(EBDC45)$: $F = I$, $H = T_3$.
$(EBDC46)$: $F = J$, $G = Z_3$.
$(EBDC47)$: $F = T_2$.
$(EBDC48)$: $F = K$.
$(EBDC49)$: $F = Z_3$.
$(EBDC50)$: $F = T_4$.
$(EBDC51)$: $F = X_3$.
$(EBDC52)$: $F = T_5$.
$(EBDC53)$: $F = Y_3$.
$(EBDC54)$: $T_1 = G$.
$(EBDC55)$: $T_1 = H$.
$(EBDC56)$: $T_1 = I$.
$(EBDC57)$: $T_1 = J$.
$(EBDC58)$: $T_1 = T_2$.
$(EBDC59)$: $T_1 = K$.
$(EBDC60)$: $T_1 = T_3$.
$(EBDC61)$: $T_1 = Z_3$.
$(EBDC62)$: $T_1 = T_4$.
$(EBDC63)$: $T_1 = X_3$.
$(EBDC64)$: $T_1 = T_5$.
$(EBDC65)$: $T_1 = Y_3$.
$(EBDC66)$: $G = H$, $T_2 = T_4$.
$(EBDC67)$: $G = I$, $T_2 = T_5$.
$(EBDC68)$: $G = J$.
$(EBDC69)$: $G = T_2$, $H = T_4$, $I = T_5$.
$(EBDC70)$: $G = T_3$.
$(EBDC71)$: $G = T_4$, $H = T_2$.
$(EBDC72)$: $G = X_3$.
$(EBDC73)$: $G = T_5$, $I = T_2$.
$(EBDC74)$: $G = Y_3$.
$(EBDC75)$: $H = K$, $J = T_5$.
$(EBDC76)$: $H = Z_3$.
$(EBDC77)$: $H = Z_3$.
$(EBDC78)$: $H = T_5$, $I = T_4$, $J = K$.
$(EBDC79)$: $H = Y_3$.
$(EBDC80)$: $I = K$, $J = T_4$.
$(EBDC82)$: $H = T_5$.
$(EBDC84)$: $J = Y_3$.
$(EBDC85)$: $J = X_3$.
$(EBDC86)$: $T_3 = T_4$.
$(EBDC87)$: $T_3 = X_3$.
$(EBDC88)$: $T_3 = T_5$.
$(EBDC89)$: $T_3 = Y_3$.
$(EBDC90)$: $T_2 = T_3$, $K = Z_3$.
$(EBDC91)$: $T_2 = Z_3$.
$(EBDC92)$: $T_2 = X_3$.
$(EBDC93)$: $T_2 = Y_3$.
$(EBDC94)$: $K = T_3$.
$(EBDC95)$: $Z_3 = T_4$.
$(EBDC96)$: $Z_3 = X_3$.
$(EBDC97)$: $Z_3 = T_5$.
$(EBDC98)$: $Z_3 = Y_3$.

Several conditions from Theorem 3.2 can be fulfilled by high-order points. However, not all these conditions will necessarily enable the attack. It is crucial to identify the specific conditions that are necessary for the attack. We will now explore the requirements case of Hessian curve.

#### *3.1.3. Special Point for Doubling on Hessian Curve*

We recall that an elliptic curve over binary fields is defined as follows:

$$E : x^3 + y^3 + 1 = 3dxy,$$

where $d \in \mathbb{K} =$.

Let $P_1 = (x_1, y_1)$ be a point on the elliptic curve $E$, in projective coordinates $P_1 = (Z_1x_1 : Z_1y_1 : Z_1)$ for some $Z \in \mathbb{K}$. Let $P_3 = (X_3 : Y_3 : Z_3) = 2P_1$.

Theorem 3.3 summarizes all conditions that a point will verify to be same-values point for doubling on elliptic curve over Hessian binary field. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for doubling on binary Hessian curves by *HBDC*.

*Theorem* 3.3. Let E be an Hessian binary elliptic curve over $\mathbb{K}$, defined by the equation $E : x^3 + y^3 + 1 = 3dxy$. The point $P = (x, y) \in E$ is a same-value point relative to the algorithm $dbl^{\mathcal{P}}$ if and only if one of the following conditions given below are satisfied:

| | | | |
|---|---|---|---|
| $x_1 = 1$ | $(HBDC1)$ | $x_1 = y_1$ | $(HBDC2)$ |
| $y_1 = 1$ | $(HBDC3)$ | $x_1 = y_1^2$ | $(HBDC4)$ |
| $x_1 = 0$ | $(HBDC5)$ | $y_1 = 1$ | $(HBDC6)$ |
| $y_1 = 0$ | $(HBDC7)$ | $x_1^2 = y_1$ | $(HBDC8)$ |
| $x_1^2 = y_1^3$ | $(HBDC9)$ | $y_1 = x^3$ | $(HBDC10)$ |
| $x_1^2 + y_1^3 = 1$ | $(HBDC11)$ | $x_1^3 + x_1^3 y_1 + y_1 = 0$ | $(HBDC12)$ |
| $x_1^2 y_1 + y_1^3 = 1$ | $(HBDC13)$ | $x_1^3 + x_1^3 y_1 + y_1^3 = 0$ | $(HBDC14)$ |
| $x_1 y_1^2 = 1$ | $(HBDC15)$ | $x_1 y_1^2 + x_1^3 = 1$ | $(HBDC16)$ |
| $x_1 y_1^3 + y_1^3 + x_1^3 = 0$ | $(HBDC17)$ | $x_1 + x_1 y_1^3 + y_1 = 0$ | $(HBDC18)$ |
| $y_1 + y_1^3 + x_1^3 = 0$ | $(HBDC19)$ | $x_1 + x_1^3 y_1 + y_1 = 0$ | $(HBDC20)$ |
| $x_1^3 + y_1^3 + x_1 = 0$ | $(HBDC21)$ | $x_1 + x_1 y_1^3 + x_1 y_1^3 + y_1 = 0$ | $(HBDC22)$ |
| $x_1 + x_1 y_1^3 + x_1^3 + y_1^3 = 0$ | $(HBDC23)$ | $x_1^3 y_1 + y_1 + y_1^3 + x_1^3 = 0$ | $(HBDC24)$ |
| $x_1^3 = y_1^2$ | $(HBDC25)$ | $x_1 = y_1^3$ | $(HBDC26)$ |
| $y_1^3 + x_1 y_1^3 + x_1 = 0$ | $(HBDC27)$ | $x_1 + x_1 y_1^3 + y_1^3 = 0$ | $(HBDC28)$ |
| $x_1^3 + y_1^2 = 1$ | $(HBDC29)$ | $x_1^2 = 1$ | $(HBDC30)$ |

*Proof.* Let $P_1 = (x_1, y_1)$ be a point on a binary Hessian elliptic curve defined by the equation $E : x^3 + y^3 + 1 = 3dxy$ over a binary field $\mathbb{K}$. In projective coordinates, we have $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1$, so the point is represented as $P_1 = (X_1 : Y_1 : Z_1) = (Z_1 x_1 : Z_1 y_1 : Z_1)$.

We analyze the intermediate variables in the point doubling algorithm $\mathbf{dbl}^{\mathcal{P}}(P_1)$ by grouping them according to the degree in $Z_1$. Let $S_i$ denote the set of terms that contain a factor $Z_1^i$. The goal is to identify all equality conditions within each $S_i$ and link them to the corresponding implications $(HBDCn)$.

From the point doubling algorithm, the following groupings are obtained:

1. $S_1 = \{Y_1 = D_1,\ Z_1 = D_2,\ X_1 = D_3\}$.
2. $S_2 = \{X_1 Z_1 = D_4,\ Z_1^2 = D_5,\ Y_1 Z_1 = D_6,\ Y_1^2 = D_7,\ X_1 Y_1 = D_8,\ X_1^2 = D_9\}$.
3. $S_4 = \{X_1^3 Z_1 = D_{10},\ X_1^3 Y_1 = D_{11},\ Y_1^3 X_1 = D_{12},\ Y_1^3 Z_1 = D_{13},\ Y_1 Z_1^3 = D_{14},\ Z_1^3 X_1 = D_{15},\ Z_1^3 X_1 - Y_1^3 X_1 = D_{16},$
$X_1^3 Y_1 - Y_1 Z_1^3 = D_{17},\ Y_1^3 Z_1 - X_1^3 Z_1 = D_{18}\}$.

Since value equalities only occur between terms of the same degree in $Z_1$, we compare terms within each set $S_i$ and obtain the following logical equivalences:

1. *Within $S_1$:*

   $D_1 = D_2 \Rightarrow (HBDC3)$

   $D_1 = D_3 \Rightarrow (HBDC2)$

   $D_2 = D_3 \Rightarrow (HBDC1)$

2. *Within $S_2$:*

   $D_4 = D_5 \Rightarrow (HBDC1)$

   $D_4 = D_6 \Rightarrow (HBDC2)$

   $D_4 = D_7 \Rightarrow (HBDC4)$

   $D_4 = D_8 \Rightarrow (HBDC5)$ and $(HBDC6)$

   $D_4 = D_9 \Rightarrow (HBDC1)$ and $(HBDC5)$

   $D_5 = D_6 \Rightarrow (HBDC3)$

   $D_5 = D_7 \Rightarrow (HBDC3)$

   $D_5 = D_8 \Rightarrow (HBDC6)$

   $D_5 = D_9 \Rightarrow (HBDC8)$

   $D_6 = D_7 \Rightarrow (HBDC3)$ and $(HBDC7)$

   $D_6 = D_8 \Rightarrow (HBDC1)$ and $(HBDC7)$

   $D_6 = D_9 \Rightarrow (HBDC8)$

   $D_7 = D_8 \Rightarrow (HBDC2)$ and $(HBDC7)$

   $D_7 = D_9 \Rightarrow (HBDC2)$

   $D_8 = D_9 \Rightarrow (HBDC2)$ and $(HBDC5)$

3. *Within $S_4$:*

   $D_{10} = D_{11} \Rightarrow (HBDC3)$ and $(HBDC5)$

   $D_{10} = D_{12} \Rightarrow (HBDC5)$ and $(HBDC9)$

   $D_{10} = D_{13} \Rightarrow (HBDC2)$

   $D_{10} = D_{14} \Rightarrow (HBDC10)$

   $D_{10} = D_{15} \Rightarrow (HBDC1)$ and $(HBDC5)$

   $D_{10} = D_{16} \Rightarrow (HBDC5)$ and $(HBDC11)$

   $D_{10} = D_{17} \Rightarrow (HBDC12)$

   $D_{10} = D_{18} \Rightarrow (HBDC7)$

   $D_{11} = D_{12} \Rightarrow (HBDC2), (HBDC5)$ and $(HBDC7)$

   $D_{11} = D_{13} \Rightarrow (HBDC7)$and $(HBDC25)$

   $D_{11} = D_{14} \Rightarrow (HBDC1)$ and $(HBDC7)$

   $D_{11} = D_{15} \Rightarrow (HBDC5)$and $(HBDC30)$

   $D_{11} = D_{16} \Rightarrow (HBDC5)$and $(HBDC13)$

   $D_{11} = D_{17} \Rightarrow (HBDC7)$

   $D_{11} = D_{18} \Rightarrow (HBDC14)$

   $D_{12} = D_{13} \Rightarrow (HBDC1)$ and $(HBDC7)$

   $D_{12} = D_{14} \Rightarrow (HBDC7)$ and $(HBDC15)$

   $D_{12} = D_{15} \Rightarrow (HBDC3)$ and $(HBDC5)$

   $D_{12} = D_{16} \Rightarrow (HBDC5)$

   $D_{12} = D_{17} \Rightarrow (HBDC7)$ and $(HBDC16)$

   $D_{12} = D_{18} \Rightarrow (HBDC17)$

   $D_{13} = D_{14} \Rightarrow (HBDC3)$ and $(HBDC7)$

   $D_{13} = D_{15} \Rightarrow (HBDC26)$

   $D_{13} = D_{16} \Rightarrow (HBDC28)$

   $D_{13} = D_{17} \Rightarrow (HBDC7)$ and $(HBDC29)$

$D_{13} = D_{18} \Rightarrow (HBDC5)$
$D_{14} = D_{15} \Rightarrow (HBDC2)$
$D_{14} = D_{16} \Rightarrow (HBDC18)$
$D_{14} = D_{17} \Rightarrow (HBDC5)$ and $(HBDC7)$
$D_{14} = D_{18} \Rightarrow (HBDC19)$
$D_{15} = D_{16} \Rightarrow (HBDC5)$ and $(HBDC7)$
$D_{15} = D_{17} \Rightarrow (HBDC20)$
$D_{15} = D_{18} \Rightarrow (HBDC21)$
$D_{16} = D_{17} \Rightarrow (HBDC22)$
$D_{16} = D_{18} \Rightarrow (HBDC23)$
$D_{17} = D_{18} \Rightarrow (HBDC24)$

After establishing the conditions under which Same Values Analysis (SVA) attacks occur during point doubling on binary elliptic curves, it is natural to investigate whether similar vulnerabilities arise in the case of point addition. Since scalar multiplication algorithms typically involve both operations, analyzing only doubling would give an incomplete picture of the attack surface. We therefore proceed to study SVA conditions for point addition, highlighting their specific algebraic structures and potential for collisions distinct from those observed in doubling.

### *3.2. Special Points of Same Values During Addition*

#### *3.2.1. Special Point for Addition on Weierstrass Curve*

This case is the result of our work [19] published at the International Cryptography Conference for Africa in 2024, abbreviated as Africacrypt 2024. Here, we provide a detailed presentation of our proofs, making them clearer and easier to understand.

Let's considere the curve:

$$E : y^2 + xy = x^3 + Ax^2 + B,$$

where $A, B \in \mathbb{K}$.

Theorem 3.4 summarizes all the conditions that must be satisfied for two points to be considered same-values points under point addition on an elliptic curve over a binary field in projective coordinates. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for addition on binary Weierstrass curves by *WBAC*.

*Theorem* 3.4. [19] Let $E$ be an elliptic curve defined by the equation $y^2 + xy = x^3 + Ax^2 + B$ over a binary field $\mathbb{K}$. The points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$ are same-values points relative to the algorithm $add^P(P_1; P_2)$ if and only if one of the following conditions is satisfied:

| | | | |
|---|---|---|---|
| $x_1 = 0$ | (WBAC1) | $x_2 = 0$ | (WBAC2) |
| $x_1 + x_2 = 0$ | (WBAC3) | $x_1 + A = 0$ | (WBAC4) |
| $x_2 = 1$ | (WBAC5) | $x_1 = 1$ | (WBAC6) |
| $y_2 = 0$ | (WBAC7) | $y_1 = 0$ | (WBAC8) |
| $y_1 + y_2 = 0$ | (WBAC9) | $x_2 = y_2$ | (WBAC10) |
| $A = 1$ | (WBAC11) | $A = 0$ | (WBAC12) |
| $x_1 + x_2 + A = 0$ | (WBAC13) | $y_2(x_1 + x_2)^2 = (y_1 + y_2)^2$ | (WBAC14) |
| $y_2 = 1$ | (WBAC15) | $y_1 = 1$ | (WBAC16) |
| $y_2 = A$ | (WBAC17) | $y_1 = A$ | (WBAC18) |
| $y_1 = x_1 + x_2 + A$ | (WBAC19) | $y_2 = x_1 + x_2 + A$ | (WBAC20) |
| $y_1 = x_1 + x_2$ | (WBAC21) | $y_2 = x_1 + x_2$ | (WBAC22) |
| $y_1 = (x_1 + x_2)^2$ | (WBAC23) | $y_2 = (x_1 + x_2)^2$ | (WBAC24) |
| $x_1 + x_2 = y_1 + y_2$ | (WBAC25) | $(x_1 + x_2)^2 = y_1 + y_2$ | (WBAC26) |
| $y_1 + y_2 = A$ | (WBAC27) | $y_1 + y_2 = 1$ | (WBAC28) |
| $(y_1 + y_2) = y_2(x_1 + x_2)$ | (WBAC29) | $(y_1 + y_2) = x_2(x_1 + x_2)$ | (WBAC30) |
| $(x_1 + x_2)^2 = (x_1 + x_2) + A$ | (WBAC31) | $(x_1 + x_2) + A = 1$ | (WBAC32) |
| $x_1 + x_2 = 1$ | (WBAC33) | $(x_1 + x_2)^2 = A$ | (WBAC34) |
| $(y_1 + y_2)^2 = x_2(x_1 + x_2)^2$ | (WBAC35) | $y_1 + y_2 = (x_1 + x_2) + A$ | (WBAC36) |
| $(y_1 + y_2)^2 + (x_1 + x_2)^2(x_1 + x_2 + A) = 0$ | (WBAC37) | | |
| $(y_1 + y_2)^2 = (x_1 + x_2)^2(x_1 + x_2 + A)$ | (WBAC38) | | |
| $(y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2) = (x_1 + x_2)^2(x_1 + x_2 + A)$ | | | (WBAC39) |
| $(y_1 + y_2) = (x_1 + x_2)(x_1 + x_2 + A)$ | | | (WBAC40) |
| $(x_1 + x_2)^2 = (y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2) + (x_1 + x_2)^2(x_1 + x_2 + A)$ | | | (WBAC41) |
| $x_2(x_1 + x_2)^2 + (y_1 + y_2)^2 + (x_1 + x_2)^2(x_1 + x_2 + A) = 0$ | | | (WBAC42) |
| $y_2(x_1 + x_2)^2 + (y_1 + y_2)^2 + (x_1 + x_2)^2(x_1 + x_2 + A) = 0$ | | | (WBAC43) |
| $x_2(x_1 + x_2)^2 = (y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2)$ | | | (WBAC44) |
| $y_2(x_1 + x_2)^2 = (y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2)$ | | | (WBAC45) |
| $(x_1 + x_2)^2 = (y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2)$ | | | (WBAC46) |
| $x_2(x_1 + x_2)^2 = (y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2) + (x_1 + x_2)^2(x_1 + x_2 + A)$ | | | (WBAC47) |

| | |
|---|---|
| $y_2(x_1+x_2)^2 = (y_1+y_2)^2 + (y_1+y_2)(x_1+x_2) + (x_1+x_2)^2(x_1+x_2+A)$ | (WBAC48) |
| $x_2(x_1+x_2)^2 = y_2(x_1+x_2)^2 + (y_1+y_2)^2 + (y_1+y_2)(x_1+x_2) + (x_1+x_2)^2(x_1+x_2+A)$ | (WBAC49) |
| $(x_1+x_2)^2 = y_2(x_1+x_2)^2 + (y_1+y_2)^2 + (y_1+y_2)(x_1+x_2) + (x_1+x_2)^2(x_1+x_2+A)$ | (WBAC50) |
| $(x_1+x_2)^2 = x_2(x_1+x_2)^2 + (y_1+y_2)^2 + (y_1+y_2)(x_1+x_2) + (x_1+x_2)^2(x_1+x_2+A)$ | (WBAC51) |
| $(y_1+y_2)[x_2(x_1+x_2)^2 + (y_1+y_2)^2 + (y_1+y_2)(x_1+x_2) + (x_1+x_2)^2(x_1+x_2+A)]$ | (WBAC52) |

*Proof.* Let $E$ be an elliptic curve defined by the equation

$$y^2 + xy = x^3 + Ax^2 + B$$

over a binary field $\mathbb{K}$. Given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) \in E$, in projective coordinates we have

$$x_1 = \frac{X_1}{Z_1}, \quad y_1 = \frac{Y_1}{Z_1^2}, \quad x_2 = \frac{X_2}{Z_2}, \quad y_2 = \frac{Y_2}{Z_2^2},$$

so that

$$P_1 = (Z_1x_1 : Z_1^2y_1 : Z_1), \quad P_2 = (Z_2x_2 : Z_2^2y_2 : Z_2).$$

We examine equalities between terms of the same degree in $Z_1$ and $Z_2$, and check for possible zero values among all terms. Let $S_{i,j}$ denote the set of expressions involving $Z_1$ to degree $i$ and $Z_2$ to degree $j$. From the point addition algorithm over binary curves, we identify the following sets:

1. $S_{1,1} = \{X_2Z_1 = S_1,\ X_1Z_2 = S_2,\ Z_1Z_2 = S_3,\ X_2Z_1 + X_1Z_2 = S_4\}$.
2. $S_{2,2} = \{Y_2Z_1^2 = S_5,\ Y_1Z_2^2 = S_6,\ Y_2Z_1^2 + Y_1Z_2^2 = S_7,\ F = S_8,\ D^2 = S_9,\ E^2 = S_{10},\ AE^2 = S_{11},\ AE^2 + F = S_{12}\}$.
3. $S_{3,3} = \{D^2B_0\}$.
4. $S_{4,4} = \{F^2 = S_{13},\ G = S_{14},\ C^2 = S_{15},\ CF = S_{16},\ C^2 + H = S_{17},\ C^2 + H + G = S_{18},\ B_0D^2E = S_{19},\ B_0D^2E + X_3 = S_{20},\ A_0D^2 = S_{21},\ A_0D^2 + X_3 = S_{22}\}$.
5. $S_{8,8} = \{Z_3J = S_{23},\ IH = S_{24},\ IH + Z_3J = S_{25}\}$.

We look equal value in the same set:

1. For the set $S_{1,1}$:
   $S_1 = S_2 \Rightarrow$ (WBAC 3), $S_1 = S_3 \Rightarrow$ (WBAC 5), $S_1 = S_4 \Rightarrow$ (WBAC 1),
   $S_2 = S_3 \Rightarrow$ (WBAC 6), $S_2 = S_4 \Rightarrow$ (WBAC 2), $S_3 = S_4 \Rightarrow$ (WBAC 33).
2. For the set $S_{2,2}$:
   (a) $S_5 = S_6 \Rightarrow$ (WBAC 9), $S_5 = S_7 \Rightarrow$ (WBAC 8), $S_5 = S_8 \Rightarrow$ (WBAC 22),
   (b) $S_5 = S_9 \Rightarrow$ (WBAC 24), $S_5 = S_{10} \Rightarrow$ (WBAC 15), $S_5 = S_{11} \Rightarrow$ (WBAC 17),
   (c) $S_5 = S_{12} \Rightarrow$ (WBAC 20), $S_6 = S_7 \Rightarrow$ (WBAC 7), $S_6 = S_8 \Rightarrow$ (WBAC 21),
   (d) $S_6 = S_9 \Rightarrow$ (WBAC 23), $S_6 = S_{10} \Rightarrow$ (WBAC 16), $S_6 = S_{11} \Rightarrow$ (WBAC 18),
   (e) $S_6 = S_{12} \Rightarrow$ (WBAC 19), $S_7 = S_8 \Rightarrow$ (WBAC 25), $S_7 = S_9 \Rightarrow$ (WBAC 26),
   (f) $S_7 = S_{10} \Rightarrow$ (WBAC 28), $S_7 = S_{11} \Rightarrow$ (WBAC 27), $S_7 = S_{12} \Rightarrow$ (WBAC 36),
   (g) $S_8 = S_9 \Rightarrow$ (WBAC 3, WBAC 33), $S_8 = S_{10} \Rightarrow$ (WBAC 33), $S_8 = S_{11} \Rightarrow$ (WBAC 13),
   (h) $S_8 = S_{12} \Rightarrow$ (WBAC 12), $S_9 = S_{10} \Rightarrow$ (WBAC 33), $S_9 = S_{11} \Rightarrow$ (WBAC 34),
   (i) $S_9 = S_{12} \Rightarrow$ (WBAC 31), $S_{10} = S_{11} \Rightarrow$ (WBAC 11), $S_{10} = S_{12} \Rightarrow$ (WBAC 32),
   (j) $S_{11} = S_{12} \Rightarrow$ (WBAC 3).
3. For the set $S_{4,4}$:
4. For the set $S_{4,4}$:

$S_{13} = S_{14} \Rightarrow$ (WBAC 3), (WBAC 32)
$S_{13} = S_{15} \Rightarrow$ (WBAC 23)
$S_{13} = S_{16} \Rightarrow$ (WBAC 3), (WBAC 23)
$S_{13} = S_{17} \Rightarrow$ (WBAC 47)
$S_{13} = S_{18} \Rightarrow$ (WBAC 41)
$S_{13} = S_{19} \Rightarrow$ (WBAC 3), (WBAC 5)
$S_{13} = S_{20} \Rightarrow$ (WBAC 51)
$S_{13} = S_{21} \Rightarrow$ (WBAC 3), (WBAC 15)
$S_{13} = S_{22} \Rightarrow$ (WBAC 50)

$S_{14} = S_{15} \Rightarrow$ (WBAC 38)
$S_{14} = S_{16} \Rightarrow$ (WBAC 3), (WBAC 40)
$S_{14} = S_{17} \Rightarrow$ (WBAC 39)
$S_{14} = S_{18} \Rightarrow$ (WBAC 7), (WBAC 25)
$S_{14} = S_{19} \Rightarrow$ (WBAC 3), (WBAC 4)
$S_{14} = S_{20} \Rightarrow$ (WBAC 44)
$S_{14} = S_{21} \Rightarrow$ (WBAC 3), (WBAC 20)
$S_{14} = S_{22} \Rightarrow$ (WBAC 45)

$S_{15} = S_{16} \Rightarrow$ (WBAC 9), (WBAC 25)
$S_{15} = S_{17} \Rightarrow$ (WBAC 3), (WBAC 9)
$S_{15} = S_{18} \Rightarrow$ (WBAC 3), (WBAC 40)
$S_{15} = S_{19} \Rightarrow$ (WBAC 35)
$S_{15} = S_{20} \Rightarrow$ (WBAC 45)
$S_{15} = S_{21} \Rightarrow$ (WBAC 14)
$S_{15} = S_{22} \Rightarrow$ (WBAC 43)

$S_{16} = S_{17} \Rightarrow$ (WBAC 9)
$S_{16} = S_{18} \Rightarrow$ (WBAC 37)
$S_{16} = S_{19} \Rightarrow$ (WBAC 3), (WBAC 30)

$S_{16} = S_{20} \Rightarrow$ (WBAC 42)
$S_{16} = S_{21} \Rightarrow$ (WBAC 3), (WBAC 29)
$S_{16} = S_{22} \Rightarrow$ (WBAC 43)

$S_{17} = S_{18} \Rightarrow$ (WBAC 3), (WBAC 32)
$S_{17} = S_{19} \Rightarrow$ (WBAC 44)
$S_{17} = S_{20} \Rightarrow$ (WBAC 3), (WBAC 4)
$S_{17} = S_{21} \Rightarrow$ (WBAC 45)
$S_{17} = S_{22} \Rightarrow$ (WBAC 20)

$S_{18} = S_{19} \Rightarrow$ (WBAC 47)
$S_{18} = S_{20} \Rightarrow$ (WBAC 2), (WBAC 3)
$S_{18} = S_{21} \Rightarrow$ (WBAC 48)
$S_{18} = S_{22} \Rightarrow$ (WBAC 3), (WBAC 7)

$S_{19} = S_{20} \Rightarrow$ (WBAC 39)
$S_{19} = S_{21} \Rightarrow$ (WBAC 3), (WBAC 10)
$S_{19} = S_{22} \Rightarrow$ (WBAC 49)

$S_{20} = S_{21} \Rightarrow$ (WBAC 49)
$S_{20} = S_{22} \Rightarrow$ (WBAC 3), (WBAC 10)

5. For the set $S_{8,8}$:
   $S_{23} = S_{24} \Rightarrow$ (WBAC 52), $S_{23} = S_{25} \Rightarrow$ (WBAC 3, WBAC 9, WBAC 47), $S_{24} = S_{25} \Rightarrow$ (WBAC 3, WBAC 48).

#### *3.2.2. Special Point for Addition on Edwards Curve*

We recall that an elliptic curve over binary fields is defined as follows:

$$E : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2,$$

where $d_1, d_2 \in \mathbb{K} = \mathbb{F}_{2^m}$, where $m$ is a positive integer.

Let $P_1 = (x_1, y_1)$, Let $P_2 = (x_2, y_2)$ be points on the elliptic curve $E$, in projective coordinates $P_1 = (Z_1x_1 : Z_1y_1 : Z_1)$, $P_2 = (Z_2x_2 : Z_2y_2 : Z_2)$ for some $Z_1, Z_2 \in \mathbb{F}_{2^m}$. Let $P_3 = (X_3 : Y_3 : Z_3) = P_1 + P_2$.

Theorem 3.5 summarizes all conditions that a point will verify to be same-values point for doubling on elliptic curve over Edwards binary field. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for adition on binary Edwards curves by *EBAC*.

*Theorem* 3.5. Let $E : d_1(x+y)+d_2(x^2+y^2) = xy+xy(x+y) + x^2y^2$ be an elliptic curve over a binary field $K = \mathbb{F}_{2^m}$, where $m$ is a positive integer. The points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$ are same-values points relative to the algorithm $add^{\mathcal{P}}(P_1; P_2)$ over Edwards binary curve if and only if one of the following conditions given below is satisfied:

| | | | |
|---|---|---|---|
| $y_1 = 1$ | $(EBAC1)$ | $x_1 = 1$ | $(EBAC2)$ |
| $x_1 = y_1$ | $(EBAC3)$ | $x_2 + y_2 = 0$ | $(EBAC4)$ |
| $d_2 = 1$ | $(WA5)$ | $x_2 + y_2 = d_1$ | $(EBAC6)$ |
| $(1 + d_2)(x_2 + y_2) = d_1$ | $(EBAC7)$ | $x_2 = 1$ | $(EBAC8)$ |
| $y_2 = 1$ | $(EBAC9)$ | $d_2x_2 + (1 + d_2)y_2 = 1$ | $(EBAC10)$ |
| $d_2y_2 + (1 + d_2)x_2 = 1$ | $(EBAC11)$ | $d_2 = 0$ | $(EBAC12)$ |
| $y_2 = 1 + d_1$ | $(EBAC13)$ | $x_2 = 1 + d_1$ | $(WA14)$ |
| $d_2x_2 + (1 + d_2)y_2 = 1 + d_1$ | $(EBAC15)$ | $d_2y_2 + (1 + d_2)x_2 = 1 + d_1$ | $(EBAC16)$ |
| $x_1^2 + x_1 = y_1^2 + y_1$ | $(EBAC17)$ | $x_1 + y_1 = 1$ | $(EBAC18)$ |
| $x_1 + y_1 = x_1(x_1 + 1)(y_2 + 1)$ | $(EBAC19)$ | | |
| $x_1 + y_1 = d_1 + y_1(y_1 + 1)(x_2 + y_2)$ | $(EBAC20)$ | | |
| $x_1 + y_1 = d_1$ | $(EBAC21)$ | $1 = x_1(x_1 + 1)(y_2 + 1)$ | $(EBAC22)$ |
| $1 = d1 + x_1(x_1 + 1)(y_2 + 1)$ | $(EBAC23)$ | $1 = d_1 + y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC24)$ |
| $x_1(x_1 + 1)(y_2 + 1) = y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC25)$ | | |
| $x_1(x_1 + 1)(y_2 + 1) = d_1 + y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC26)$ | | |
| $x_1(x_1 + 1)(y_2 + 1) = d_1$ | $(EBAC27)$ | $d_2(x_2 + y_2) = d_1$ | $(EBAC28)$ |
| $d_1 + y_1(y_1 + 1)(x_2 + 1) = 0$ | $(EBAC29)$ | $x_1 + y_1 = y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC30)$ |
| $x_1 + y_1 = y_1(y_1 + 1)(x_2 + 1) + d_1$ | $(EBAC31)$ | $1 = y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC32)$ |
| $1 = d_1$ | $(EBAC33)$ | | |
| $y_1 = 0$ | $(EBAC34)$ | $(x_1 + y_1)(d_1 + d_2(x_2 + y_2)) = 1$ | $(EBAC35)$ |
| $1 = x_2(d_1 + x_1(x_1 + 1)(y_2 + 1)$ | $(EBAC36)$ | $1 = y_2(d_1 + y_1(y_1 + 1)(x_2 + 1)$ | $(EBAC37)$ |
| $(x_1 + y_1)(d_2(x_2 + y_2) + d_1) + x_2(d_1 + x_1(x_1 + 1)(y_2 + 1) = 1$ | | | $(EBAC38)$ |
| $(x_1 + y_1)(d_2(x_2 + y_2) + d_1) + y_2(d_1 + y_1(y_1 + 1)(x_2 + 1) = 1$ | | | $(EBAC39)$ |
| $(x_1 + y_1)(d_2(x_2 + y_2) + d_1) = d_1$ | $(EBAC40)$ | $y_1(y_1 + 1)(x_2 + y_2) = 1$ | $(EBAC41)$ |
| $x_1(x_1 + 1)(x_2 + y_2) = 1$ | $(EBAC42)$ | $y_1(y_1 + 1)(x_2 + y_2) + d_1 = 1$ | $(EBAC41)$ |

| | | | |
|---|---|---|---|
| $x_1(x_1+1)(x_2+y_2)+d_1=1$ | $(EBAC44)$ | $x_1(x_1+1)(x_2+y_2)=d_1$ | $(EBAC45)$ |
| $y_1(y_1+1)(x_2+y_2)=d_1$ | $(EBAC46)$ | $x_1=0$ | $(EBAC47)$ |
| $x_2(d_1+x_1(x_1+1)(y_2+1)=d_1$ | | | $(EBAC48)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)+y_2(d_1+y_1(y_1+1)(y_2+1)=d_1$ | | | $(EBAC49)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)+x_2(d_1+x_1(x_1+1)(y_2+1)=d_1$ | | | $(EBAC50)$ |
| $y_2(d_1+y_1(y_1+1)(x_2+1)=d_1$ | $(EBAC51)$ | $x_2=0$ | $(EBAC52)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)=y_1(y_1+1)(x_2+y_2)$ | | | $(EBAC53)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)+y_1(y_1+1)(x_2+y_2)=d_1$ | | | $(EBAC54)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)=x_1(x_1+1)(1+y_2)$ | | | $(EBAC55)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)+x_1(x_1+1)(1+y_2)=d_1$ | | | $(EBAC56)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)=x_2(d_1+x_1(x_1+1)(y_2+1)$ | | | $(EBAC57)$ |
| $(x_1+y_1)(d_2(x_2+y_2)+d_1)=y_2(d_1+x_1(x_1+1)(y_2+1)$ | | | $(EBAC58)$ |
| $y_2=0$ | $(EBAC59)$ | $x_1(x_1+1)(x_2+y_2)=y_1(y_1+1)(x_2+y2)+d_1$ | $(EBAC60)$ |

| | |
|---|---|
| $x_1(x_1+1)(x_2+y_2)=x_2(d_1+x_1(x_1+1)(x_2+y_2))$ | $(EBAC61)$ |
| $x_1(x_1+1)(x_2+y_2)=x_2(d_1+x_1(x_1+1)(x_2+y_2))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC62)$ |
| $x_1(x_1+1)(x_2+y_2)=y_2(d_1+y_1(y_1+1)(x_2+y_2))$ | $(EBAC63)$ |
| $x_1(x_1+1)(x_2+y_2)=y_2(d_1+y_1(y_1+1)(x_2+y_2))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC64)$ |
| $d_1+x_1(x_1+1)(x_2+y_2)=x_2(d_1+x_1(x_1+1)(y_2+1))$ | $(EBAC65)$ |
| $d_1+x_1(x_1+1)(x_2+y_2)=x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC66)$ |
| $d_1+x_1(x_1+1)(x_2+y_2)=y_2(d_1+y_1(y_1+1)(x_2+1))$ | $(EBAC67)$ |
| $d_1+x_1(x_1+1)(x_2+y2)=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC68)$ |
| $d_1+x_1(x_1+1)(x_2+y_2)=y_2(d_1+y_1(y_1+1)(x_2+1))$ | $(EBAC67)$ |
| $d_1+x_1(x_1+1)(x_2+y2)=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC68)$ |
| $y_1(y_1+1)(y_2+x_2)+d_1=x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC70)$ |
| $y_1(y_1+1)(y_2+x_2)+d_1=y_2(d_1+y_1(y_1+1)(x_2+1))$ | $(EBAC71)$ |
| $y_1(y_1+1)(y_2+x_2)+d_1=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC72)$ |
| $x_2(d_1+x_1(x_1+1)(y_2+1))=y_2(d_1+y_1(y_1+1)(x_2+1))$ | $(EBAC73)$ |
| $x_2(d_1+x_1(x_1+1)(y_2+1))=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC74)$ |
| $y_1(d_1+x_1(x_1+1)(x_2+y_2))=x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC75)$ |
| $[x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)][d_1+y_1(y_1+1)(x_2+y_2)]$ $=[d_1+x_1(x_1+1)(x_2+y_2)][y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)]$ | $(EBAC76)$ |
| $x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)=x_1(d_1+x_1(x_1+1)(x_2+y_2)$ | $(EBAC77)$ |
| $[x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)][d_1+y_1(y_1+1)(x_2+y_2)]$ $=[d_1+x_1(x_1+1)(x_2+y_2)][y_2(d_1+y_1(y_1+1)(x_2+1))$ $+(x_1+y_1)(d_2(x_2+y_2)+d_1)]+x_1(d_1+x_1(x_1+1)(x_2+y_2)$ | $(EBAC78)$ |
| $x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)=(d_1+x_1(x_1+1)(x_2+y_2)$ | $(EBAC79)$ |
| $y_1(d_1+y_1(y_1+1)(x_2+y_2)=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC80)$ |
| $[d_1+x_1(x_1+1)(x_2+y_2][d_1+y_1(y_1+1)(x_2+y_2)]y_1$ $=[d_1+x_1(x_1+1)(x_2+y_2)][y_2(d_1+y_1(y_1+1)(x_2+1))$ $+(x_1+y_1)(d_2(x_2+y_2)+d_1)]+x_1(d_1+x_1(x_1+1)(x_2+y_2)$ | $(EBAC81)$ |
| $y_1[x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)]$ $=[y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)]$ | $(EBAC82)$ |
| $y_1[x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)]=x_1$ | $(EBAC83)$ |
| $y_1[x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)]=$ $[d_1+x_1(x_1+1)(x_2+y_2)][y_2(d_1+y_1(y_1+1)(x_2+1))+$ $(x_1+y_1)(d_2(x_2+y_2)+d_1)]+x_1(d_1+x_1(x_1+1)(x_2+y_2)$ | $(EBAC84)$ |
| $y_1(y_1+1)(y_2+x_2)=x_2(d_1+x_1(x_1+1)(y_2+1))$ | $(EBAC85)$ |
| $y_1(y_1+1)(y_2+x_2)=x_2(d_1+x_1(x_1+1)(y_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC86)$ |
| $y_1(y_1+1)(y_2+x_2)=y_2(d_1+y_1(y_1+1)(x_2+1))$ | $(EBAC87)$ |
| $y_1(y_1+1)(y_2+x_2)=y_2(d_1+y_1(y_1+1)(x_2+1))+(x_1+y_1)(d_2(x_2+y_2)+d_1)$ | $(EBAC88)$ |

*Proof.* Let $E$ be an elliptic curve defined over the binary field $\mathbb{K}$, where $m$ is a positive integer, by the equation

$$d_1(x+y)+d_2(x^2+y^2)=xy+xy(x+y)+x^2y^2.$$

Consider points $P_1=(x_1,y_1)$ and $P_2=(x_2,y_2)$ on $E$. In projective coordinates, we write

$$x_1=\frac{X_1}{Z_1},\quad y_1=\frac{Y_1}{Z_1},\quad x_2=\frac{X_2}{Z_2},\quad y_2=\frac{Y_2}{Z_2},$$

so that
$P_1=(X_1:Y_1:Z_1)=(Z_1x_1:Z_1y_1:Z_1)$,
$P_2=(X_2:Y_2:Z_2)=(Z_2x_2:Z_2y_2:Z_2)$.

Our goal is to verify equalities between terms sharing the same degrees in $Z_1$ and $Z_2$, and identify terms that vanish.

Define $S_{i,j}$ as the set of terms involving $Z_1$ to the power $i$ and $Z_2$ to the power $j$. From the point addition algorithm on the binary Edwards curve, we have the following sets:

$$S_{1,0}=\{W_1,T_0,T_1\}$$

$$S_{0,1}=\{W_2,T_3,T_4,T_5,T_{10},T_{18}\}$$

$$S_{2,0}=\{A,B\},\quad S_{0,2}=\{D\},\quad S_{1,1}=\{C\},$$

$$S_{2,1}=\{T_6,T_7,T_{11},T_{19},T_{20},I\}$$

$$S_{2,2}=\{T_2,E,H,T_8,T_9,U,V,T_{13},T_{14},T_{21},T_{22}\}$$

$$S_{3,2}=\{T_{15},T_{23}\},\quad S_{4,4}=\{S\},$$

$$S_{5,4}=\{T_{16},T_{17},X_3,T_{24},T_{25},Y_3,Z_3\}$$

Note that equalities can only occur between terms within the same set $S_{i,j}$. To identify these equalities, we compare pairs of terms within each subset, yielding the following conditions:

(EBAC1) $W_1=T_0, T_{20}=I, E=V$
(EBAC2) $W_1=T_1, T_{12}=I, E=U$
(EBAC3) $T_1=T_0, T_{13}=T_{14}, T_{21}=T_{22}$
(EBAC4) $W_2=T_3, T_4=T_5, T_{10}=T_{18}, E=U=V$, $T_8=T_9$
(EBAC5) $W_2=T_3$
(EBAC6) $W_2=T_4$
(EBAC7) $W_2=T_5$
(EBAC8) $W_2=T_{10}, T_{20}=I$
(EBAC9) $W_2=T_{18}, T_{12}=I$
(EBAC10) $T_2=T_{10}$
(EBAC11) $T_3=T_{18}$
(EBAC12) $T_4=T_5$
(EBAC13) $T_4=T_{10}$
(EBAC14) $T_4=T_{18}$
(EBAC15) $T_5=T_{10}$
(EBAC16) $T_5=T_{18}$
(EBAC17) $A=B, U=V, T_8=T_9$
(EBAC18) $T_6=T_7$
(EBAC19) $T_6=T_{11}$
(EBAC20) $T_6=T_{12}$
(EBAC21) $T_6=I$
(EBAC22) $T_7=T_{11}$
(EBAC23) $T_7=T_{12}$
(EBAC24) $T_7=T_{24}$
(EBAC25) $T_{11}=T_{19}, T_{12}=T_{20}$
(EBAC26) $T_{11}=T_{20}, T_{12}=T_{19}$
(EBAC27) $T_{11}=I, T_{21}=T_{22}$
(EBAC28) $T_3=T_4, T_{13}=T_{14}$
(EBAC29) $T_{19}=I, H=T_{22}$
(EBAC30) $T_6=T_{19}$
(EBAC31) $T_6=T_{20}$
(EBAC32) $T_7=T_{19}$
(EBAC33) $T_7=I$
(EBAC34) $E=V$
(EBAC35) $T_2=H$
(EBAC36) $T_2=T_{13}$
(EBAC37) $T_2=T_{21}$
(EBAC38) $T_2=T_{14}$
(EBAC39) $T_2=T_{22}$
(EBAC40) $E=H$
(EBAC41) $T_2=T_9$
(EBAC42) $T_2=T_8$
(EBAC43) $T_2=V$
(EBAC44) $T_2=U$
(EBAC45) $T_8=E$
(EBAC46) $T_9=E$
(EBAC47) $E=U$
(EBAC48) $T_{13}=E$
(EBAC49) $T_{22}=E$
(EBAC50) $T_{14}=E$
(EBAC51) $T_{21}=E$
(EBAC52) $T_{14}=H$
(EBAC53) $T_9=H$
(EBAC54) $H=V$
(EBAC55) $T_8=H$
(EBAC56) $H=U$
(EBAC57) $T_{13}=H$
(EBAC58) $T_{21}=H$
(EBAC59) $T_{22}=H$
(EBAC60) $T_8=V, T_9=U$
(EBAC61) $T_8=T_{13}$
(EBAC62) $T_8=T_{14}$
(EBAC63) $T_8=T_{21}$
(EBAC64) $T_8=T_{22}$
(EBAC65) $T_{21}=U$
(EBAC66) $T_{14}=U$
(EBAC68) $T_{22}=U$
(EBAC69) $T_{13}=V$
(EBAC70) $T_{14}=V$
(EBAC71) $T_{21}=V$
(EBAC72) $T_{22}=V$
(EBAC73) $T_{13}=T_{21}, T_{14}=T_{22}$
(EBAC74) $T_{13}=T_{22}, T_{14}=T_{21}$
(EBAC75) $T_{16}=T_{17}$
(EBAC76) $T_{16}=T_{24}$
(EBAC77) $T_{16}=T_{25}$
(EBAC78) $T_{16}=Y_3$
(EBAC79) $T_{16}=Z_3$
(EBAC80) $T_{17}=T_{24}$

(EBAC81) $T_{17} = Y_3$
(EBAC82) $X_3 = T_{24}$
(EBAC83) $X_3 = T_{25}$
(EBAC84) $X_3 = Y_3$
(EBAC85) $T_9 = T_{13}$
(EBAC86) $T_9 = T_{14}$
(EBAC87) $T_9 = T_{21}$
(EBAC88) $T_9 = T_{22}$

### *3.2.3. Special Point for Addition on Hessian Curve*

We recall that an elliptic curve over binary fields is defined as follows:

$$E : x^3 + y^3 + 1 = 3dxy$$

, where $d \in \mathbb{K}$.

Let $P_1 = (x_1, y_1)$, Let $P_2 = (x_2, y_2)$ be points on the elliptic curve $E : x^3+y_3+1 = 3dxy$, in projective coordinates $P_1 = (Z_1x_1 : Z_1y_1 : Z_1)$, $P_2 = (Z_2x_2 : Z_2y_2 : Z_2)$ for some $Z_1, Z_2 \in \mathbb{K}$. Let $P_3 = (X_3 : Y_3 : Z_3) = P_1 + P_2$.

Theorem 3.6 summarizes all conditions that a point will verify to be same-values point for doubling on elliptic curve over Hessian binary fields. We denote the conditions that a point must satisfy to ensure at least two identical intermediate values for addition on binary Hessian curves by ***HBAC***.

*Theorem* 3.6. Let $E : x^3 + y^3 + 1 = 3dxy$ be an elliptic curve over a binary field $\mathbb{K}$. The points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$ are same-values points relative to the algorithm $add^{\mathcal{P}}(P_1; P_2)$ over Hessian binary curve if and only if one of the following conditions given below is satisfied:

| | | | |
|---|---|---|---|
| $x_1 = 0$ | $(HBAC1)$ | $x_1 = y_2$ | $(HBAC2)$ |
| $x_1 = y_1$ | $(HBAC3)$ | $y_2 = 0$ | $(HBAC4)$ |
| $x_1 = 1$ | $(HBAC5)$ | $x_1 = x_2$ | $(HBAC6)$ |
| $x_1y2 = x_2$ | $(HBAC7)$ | $x_1y_2 = x_2y_1$ | $(HBAC8)$ |
| $x_{1l}y_2 = y_1$ | $(HBAC9)$ | $x_2 = y_2$ | $(HBAC10)$ |
| $y_2 = x_2y_1$ | $(HBAC11)$ | $x_2 = 0$ | $(HBAC12)$ |
| $y_1 = 1$ | $(HBAC13)$ | $x_2 = y_1$ | $(HBAC14)$ |
| $y_1 = 0$ | $(HBAC15)$ | $x_2 = 1$ | $(HBAC16)$ |
| $x_1 = x_2y_1$ | $(HBAC17)$ | $x_1 = x_2^{[}2]$ | $(HBAC18)$ |
| $x_1y_1 = x_2y_2$ | $(HBAC19)$ | $y_1 = y_2^2$ | $(HBAC20)$ |
| $x_1y_1 - x_1^2y_2 + x_2^2y_1 = 0$ | $(HBAC21)$ | $x_1y_1 - y_1^2x_2 + y_2^2x_1 = 0$ | $(HBAC22)$ |
| $y_1^2 = y_2$ | $(HBAC23)$ | $x_2y_1^2 = x_1y_2^2$ | $(HBAC24)$ |
| $1\, x_2y_12 = x_1^2y_2$ | $(HBAC25)$ | $x_2y_1^2 - x_1^2y_2 + x_2^2y_1 = 0$ | $(HBAC26)$ |
| $x_2y_1^2 - x_2y_2 + x_1y_1 = 0$ | $(HBAC27)$ | $y_2 = 1$ | $(HBAC28)$ |
| $x_2^2y_1 = x_1y_2^2$ | $(HBAC29)$ | $x_2^2y_1 = x_1^2y_2$ | $(HBAC30)$ |
| $x_2y_2 - x_1y_1 - x_1^2y_2 = 0$ | $(HBAC31)$ | $x_2^2y_1 - y_1^2x_2 + y_2^2x_1 = 0$ | $(HBAC32)$ |
| $x_2^2y_1 - x2y_2 + x_1y_1 = 0$ | $(HBAC33)$ | $x_2y_1^2 - x_1y_2^2 - x_2y_2 + x_1y_1 = 0$ | $(HBAC34)$ |
| $x_2 = x_1^2$ | $(HBAC35)$ | $x_2y_2 - x_1^2y_2 + x_2^2y_1 = 0$ | $(HBAC36)$ |
| $x_2y_2 - x2y_1^2 + x_1y_2^2 = 0$ | $(HBAC37)$ | $y_2 = x_1$ | $(HBAC38)$ |
| $x_1y_2^2 - x_1^2y_2 + x_2^2y_1 = 0$ | $(HBAC39)$ | $x_1y_2^2 - x2y_2 + x_1y_1 = 0$ | $(HBAC40)$ |
| $x_1^2y_2 - x_2y_1^2 + x_1y_2^2 = 0$ | $(HBAC41)$ | $x_1^2y_2 - x_2^2y_1 - x_2y_1^2 + x_1y_2^2 = 0$ | $(HBAC42)$ |
| $x_1^2y_2 - x_2^2y_1 - x_2y_2 + x_1y_1 = 0$ | $(HBAC43)$ | $y_1 = y_2$ | $(HBAC44)$ |

Proof. Let $E$ be an elliptic curve defined by the equation $E : x^3 + y_3 + 1 = 3dxy$ over a binary field $\mathbb{K}$. Given points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$, in projective coordinates $x_1 = X_1/Z_1$, $y_1 = Y_1/Z_1$, $x_2 = X_2/Z_2$, $y_2 = Y_2/Z_2$, in projective coordinates $P_1 = (X_1 : Y_1 : Z_1) = (Z_1x_1 : Z_1y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2) = (Z_2x_2 : Z_2y_2 : Z_2)$ we have to check equalities between terms with the same degree of $Z_1$ and $Z_2$, and zero values between all terms. Let $S_{i,j}$ denote the set of values which involve a term $Z_1$ with a degree $i$ and $Z_2$ with a degree $j$. When we look at the algorithm for point adding in binary curve, we have:

1. $S_{1,1} = \{X_1Z_2 = A_1, X_1Y_2 = A_2, Y_2Z_1 = A_3, X_2Z_1 = A_4, X_2Y_1 = A_5, Y_1Z_2 = A_6\}$.
2. $S_{2,2} = \{X_1Y_1Z_2^2 = A_7, X_2Y_1^2Z_1 = A_8, X_2^2Y_1Z_1 = A_9, X_2Y_2Z_1^2 = A_{10}, X_1Y_2^2Z_1 = A_{11}, X_1^2Y_2Z_2 = A_{12}, X_1^2Y_2 - X_2^2Y_1 = A_{13}, X_2Y_1^2 - X_1Y_2^2 = A_{14}, X_2Y_2 - X_1Y_1 = A_{15}\}$

Identical values can only be identified within the same set. To locate them, we compare the terms within each subset pairwise:

1. For the set $S_{1,1}$:
   $A_1 = A_2 \Rightarrow$ (HBAC1) and $(HBAC28)$.
   $A_1 = A_3 \Rightarrow$ ( HBAC2)
   $A_1 = A_4 \Rightarrow$ (HBAC6)
   $A_1 = A_5 \Rightarrow$ ( HBAC 17)
   $A_1 = A_6 \Rightarrow$ (HBAC3)
   $A_2 = A_3 \Rightarrow$ ( HBAC4) and $(HBAC5)$
   $A_2 = A_4 \Rightarrow$ ( HBAC7)
   $(A_2 = A_5 \Rightarrow$ ( HBAC8)
   $A_2 = A_6 \Rightarrow$ ( HBAC9).
   $A_3 = A_4 \Rightarrow$ ( HBAC 10)
   $A_3 = A_5 \Rightarrow$ ( HBAC 11).
   $A_3 = A_6 \Rightarrow$ ( HBAC 44).
   $A_4 = A_5 \Rightarrow$ ( HBAC 12) and $(HBAC13)$.

$A_4 = A_6 \Rightarrow$ ( HBAC 14).
$A_5 = A_6 \Rightarrow$ ( HBAC15) and $(HBAC16)$.

2. For the set $S_{2,2}$:
$A_7 = A_8 \Rightarrow$ ( HBAC15) and $(HBAC17)$.
$A_7 = A_9 \Rightarrow$ ( HBAC15) and $(HBAC18)$.
$A_7 = A_{10} \Rightarrow$ ( HBAC 19)
$A_7 = A_{11} \Rightarrow$ ( HBAC 1) and $(HBAC20)$.
$A_7 = A_{12} \Rightarrow$ ( HBAC1) and $(HBAC9)$.
$A_7 = A_{13} \Rightarrow$ ( HBAC 21)
$A_7 = A_{14} \Rightarrow$ ( HBAC 22).
$A_7 = A_{15} \Rightarrow$ ( HBAC4) and $(HBAC12)$.
$A_8 = A_9 \Rightarrow$ ( HBAC12) , $(HBAC14)$ and $(HBAC15)$.
$A_8 = A_{10} \Rightarrow$ ( HBAC8), $(HBAC12)$ and $(HBAC23)$.
$A_8 = A_{11} \Rightarrow$ ( HBAC 24).
$A_8 = A_{12} \Rightarrow$ ( HBAC25).
$A_8 = A_{13} \Rightarrow$ ( HBAC26).
$A_8 = A_{14} \Rightarrow$ ( HBAC1) and $(HBAC4)$.
$A_8 = A_{15} \Rightarrow$ ( HBAC27).
$A_9 = A_{10} \Rightarrow$ ( HBAC11), and $(HBAC12)$.
$A_9 = A_{11} \Rightarrow$ ( HBAC29).
$A_9 = A_{12} \Rightarrow$ ( HBAC30)
$A_9 = A_{13} \Rightarrow$ ( HBAC1) and $(HBAC4)$.
$A_9 = A_{14} \Rightarrow$ ( HBAC32).
$A_9 = A_{15} \Rightarrow$ ( HBAC33).
$A_{10} = A_{11} \Rightarrow$ ( HBAC4) and $(HBAC7)$.
$A_{10} = A_{12} \Rightarrow$ ( HBAC4) and $(HBAC35)$.
$A_{10} = A_{13} \Rightarrow$ ( HBAC36).
$A_{10} = A_{14} \Rightarrow$ ( HBAC37).
$A_{10} = A_{15} \Rightarrow$ ( HBAC1) and $(HBAC15)$.
$A_{11} = A_{12} \Rightarrow$ ( HBAC1), $(HBAC4)$ and $(HBAC38)$.
$A_{11} = A_{13} \Rightarrow$ ( HBAC39).
$A_{11} = A_{14} \Rightarrow$ ( HBAC12) and $(HBAC15)$.
$A_{11} = A_{15} \Rightarrow$ ( HBAC40).
$A_{12} = A_{13} \Rightarrow$ ( HBAC12) and $(HBAC15)$.
$A_{12} = A_{14} \Rightarrow$ ( HBAC41).
$A_{12} = A_{15} \Rightarrow$ ( HBAC31).
$A_{13} = A_{14} \Rightarrow$ ( HBAC42).
$A_{13} = A_{15} \Rightarrow$ ( HBAC43).
$A_{14} = A_{15} \Rightarrow$ ( HBAC34).

The different theorems of this work summarize the conditions that points must verify to admit at least two identical intermediate values during the addition or doubling of points on the considered curve model. However, very few of these conditions are useful for the SVA attack, it is a question of currently searching for these conditions which will allow to obtain the collision

### *3.3. Collision Power Analysis*

#### *3.3.1. Collision over Weierstrass Curve*

This case is the result of our article in Africacript 2024 [19].
In the case of binary Weierstrass curves, we have listed in Theorems 3.1 and 3.4 the conditions for obtaining points with the same values. Only a few of these conditions guarantee collision. We recall that collision occurs when the same operation on scalars is repeated several times with the same inputs. The scalar operations thus considered will be doubling and raising to the square. Taking into account all these principles we summarize the collision conditions in the case of binary Weierstrass curves

1. *(WBDC2):* $x_1 = 1$. This ensures that the squaring operations on lines 3 and 6 of $dbl^{\mathcal{P}}$ over Weierstrass curve produce the same power consumption.
2. *(WBDC5):* $x_1^4 = B$. This results in identical power traces for the squaring operations on lines 5 and 8 of $dbl^{\mathcal{P}}$ over Weierstrass curve.
3. *(WBDC7):* $y_1^2 = B$. The squaring computations on lines 5 and 10 of $dbl^{\mathcal{P}}$ over Weierstrass curve yield the same power consumption.
4. *(WBDC17):* $x_1^2 = y_1$. This condition aligns the squaring operations on lines 8 and 10 of $dbl^{\mathcal{P}}$ over Weierstrass curve in terms of power usage.
5. *(WA25):* $x_1 + x_2 = y_1 + y_2$. This equality implies equal power consumption during the squaring operations on lines 12 and 18 of $add^{\mathcal{P}}$ over Weierstrass curve.
6. *(WA33):* $x_1 + x_2 = 1$. The squaring operations on lines 13 and 14 of $add^{\mathcal{P}}$ over Weierstrass curve will consume equal amounts of power.

#### *3.3.2. Collision over Edwards Curve*

*Collision Power Analysis:* Among all conditions of Theorem 3.2 and Theorem 3.5, the conditions below give the collision are:

1. *(EBDC1):* $x = y$, this condition implies that the power consumption during the computation of the *square* at the lines 1 and 3 of $dbl^{\mathcal{P}}$ over Edwards curve are the same.
2. *(EBDC2)* $x = 1$, this condition implies that the power consumption during the computation of the *square* at the lines 1 and 5 of $dbl^{\mathcal{P}}$ over Edwards curve are the same.
3. *(EBDC17)* $y = 1$, this condition implies that the power consumption during the computation of the *square* at the lines 3 and 5 of $dbl^{\mathcal{P}}$ over Edwards curve are the same.

#### *3.3.3. Collision over Hessian Curve*

*Collision Power Analysis:* Among all conditions of Theorem 3.6 and Theorem 3.3, the collision are guaranteed:

1. *(HBDC1):* $x = 1$, this condition implies that the power consumption during the computation of the *square* at the lines 6 and 10 of $dbl^{\mathcal{P}}$ over binary Hessian are the same.
2. *(HBDC2)* $x = y$, this condition implies that the power consumption during the computation of the *square* at the lines 8 and 10 of $dbl^{\mathcal{P}}$ over binary Hessian are the same.
3. *(HBDC3):* $y = 1$, this condition implies that the power consumption during the computation of the *square* at the lines 6 and 8 of $dbl^{\mathcal{P}}$ over binary Hessian are the same.

Let us now look at the effectiveness of this attack on the curves recommended by NIST and SECG.

# 4. Same Values Analysis on Standard Curve on Binary Fields

This section is the result of our article in Africacript 2024 [19].

Like in [8] where the authors investigated zero-value points on recommended curves defined over fields of odd characteristic, in [9] where the authors investigated zero-value points on recommended curves defined over binary fields , in [10]The authors investigated same-value points on recommended curves defined over fields of odd characteristic, we will look at the intermediate value points on the recommended curves in the cases of doubling exclusively. On binary fields, the curves recommended by NIST and SECG are defined only in the case of Weierstrass binary curves

1. the roots of the polynomial $P(x) = x - 1$ are the x-coordinates of the points satisfying the collision condition *(WBDC2)*.
2. the roots of the polynomial $x_1^4 = B$ are the x-coordinates of the points satisfying the collision condition *(WBDC5)*.
3. the roots of the polynomial $L(x) = x^3 + Ax^2 - B^{2^{m-1}}x$ are the x-coordinates of the points satisfying the collision condition *(WBDC7)*
4. the roots of the polynomial $M(x) = x^4 - Ax^2 - B$. are the x-coordinates of the points satisfying the collision condition *(WBDC17)*

We needed SageMath to find these special points on the recommended curves. The principle of our code is to search for the solutions of these polynomials and then find the intersections with the different curves.

For example the *SECG* recommended curve *sect131r1* give as $E : y^2 + xy = x^3 + Ax^2 + B$ over a binary field $K = \mathbb{F}_{2^m}$ where :
$A = 0x07a11b09a76b562144418ff3ff8c2570b8$,
$B = 0x0217c05610884b63b9c6c7291678f9d341$
$m = 131$, the curve order is $n = 0x040000000000000000023123953a9464b54d$,
the generator of the curve is the point $G$ such that $X_G = 0x0081baf91fdf9833c40f9c181343638399$, $Y_G = 0x078c6e7ea38c001f73c8134b1b4ef9e150$. All these values are in hexadecimal.

1. Points of the curve solution of $P = x^2 - 1$
   (a) $P_1 = (1 : \texttt{C3114B3003A73C05CC3086D600A6C2EC8} : 1)$
   (b) order of $P_1$ = 27222589353675077077686810712579939099 80
2. Points of the curve solution of $Q = x^4 - B$:
   (a) $P_2 = (X, Y, Z)$ with

$$X = \texttt{6086CC0000000000000000000000000000000FFFE0C0001C001F}$$
$$Y = \texttt{3007988000000000000000000000000000007F800C0003C104D}$$
$$Z = \texttt{00000000000000000000000000000001}$$

   (b) order of $P_2$ = 4
3. Points of the curve solution of $M = x^4 - A * x^2 - B$:
   No solution for the polynomial M
4. Points of the curve solution of $N = x^4 - 2 * x^3 - A * x^2 - B$:
   No solution for the polynomial N

We summarize in Table 7 and Table 8 our study of the SVA attack on recommended curves. In these different tables, we have mentioned all the collision conditions and have used the following notations. '$\oplus$' to signify that the curve has a same-values point of large order, '$\odot$' to signify that the curve has a same-values point of small order, '$\otimes$' to signify that the curve do not have a same-values point which satisfy the condition aboved $\oplus$, $\odot$ are use if some point have large order and the others have small. We also mentioned the execution time for each curve with our computer Intel core I7-6600UCPU@ 2.60GHZ with 19GiB of RAM.

***Table 7.*** *SECG curves over $\mathbb{F}_{2^m}$ and SVA points from dbl - $\mathbb{F}_{2^m}$,where $m$ is a positive integer.*

| Name of Curve | $\mathbf{x = 1}$ | $\mathbf{x^4 = B}$ | $\mathbf{y^2 = B}$ | $\mathbf{x^2 = y}$ | Curve Order | Execution Time |
|---|---|---|---|---|---|---|
| $sect113r1$ | $\oplus$ | $\otimes$ | $\oplus, \odot$ | $\oplus$ | $2 \times n$ | 0.1656479835510254 |
| $sect113r2$ | $\oplus$ | $\otimes$ | $\oplus, \odot$ | $\otimes$ | $2 \times n$ | 0.11415243148803711 |
| $sect131r1$ | $\oplus$ | $\odot$ | $\oplus, \odot$ | $\otimes$ | $2 \times n$ | 0.27272844314575195 |

| Name of Curve | $\mathbf{x=1}$ | $\mathbf{x^4=B}$ | $\mathbf{y^2=B}$ | $\mathbf{x^2=y}$ | Curve Order | Execution Time |
|---|---|---|---|---|---|---|
| $sect131r2$ | $\otimes$ | $\odot$ | $\odot$ | $\otimes$ | $2\times n$ | 0.09245753288269043 |
| $sect163k1$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $4\times n$ | 0.06290864944458008 |
| $sect163r1$ | $\otimes$ | $\otimes$ | $\odot$ | $\oplus$ | $2\times n$ | 0.20116949081420898 |
| $sect163r2$ | $\otimes$ | $\otimes$ | $\oplus,\odot$ | $\otimes$ | $2\times n$ | 0.1479189395904541 |
| $sect193r1$ | $\oplus$ | $\odot$ | $\oplus,\odot$ | $\otimes$ | $2\times n$ | 0.4444913864135742 |
| $sect193r2$ | $\oplus$ | $\otimes$ | $\oplus,\odot$ | $\otimes$ | $2\times n$ | 0.380489577838135 |
| $sect233k1$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.23964238166809082 |
| $sect233r1$ | $\oplus$ | $\otimes$ | $\odot$ | $\oplus$ | $2\times n$ | 1.6709847450256348 |
| $sect239k1$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.22464609146118164 |
| $sect283k1$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.1726086139678955 |
| $sect283r1$ | $\oplus$ | $\odot$ | $\odot$ | $\odot$ | $2\times n$ | 1.0795626640319824 |
| $sect409r1$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $2\times n$ | 0.3824753761291508 |
| $sect409k1$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.20759129524230957 |
| $sect571k1$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.8523068428039551 |
| $sect571r1$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $2\times n$ | 1.0717732906341553 |

***Table 8.*** *NIST curves over $\mathbb{F}_{2^m}$ and SVA points from dbl - $\mathbb{F}_{2^m}$,where $m$ is a positive integer.*

| Name of Curve | $\mathbf{x=1}$ | $\mathbf{x^4=B}$ | $\mathbf{y^2=B}$ | $\mathbf{x^2=y}$ | Curve Order | Execution Time |
|---|---|---|---|---|---|---|
| $K-163$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $2\times n$ | 055924415588378906 |
| $B-163$ | $\otimes$ | $\otimes$ | $\oplus,\odot$ | $\otimes$ | $2\times n$ | 0.20136809349060059 |
| $B-233$ | $\oplus$ | $\otimes$ | $\odot$ | $\oplus$ | $2\times n$ | 1.7690699100494385 |
| $K-233$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.16431379318237305 |
| $B-283$ | $\oplus$ | $\otimes$ | $\oplus$ | $\oplus$ | $2\times n$ | 1.126676321029663 |
| $K-283$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.2727367877960205 |
| $B-409$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $2\times n$ | 0.3601799011230469 |
| $K-409$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $4\times n$ | 0.31488513946533203 |
| $B-571$ | $\otimes$ | $\otimes$ | $\odot$ | $\otimes$ | $2\times n$ | 0.2166743278503418 |
| $K-571$ | $\odot$ | $\odot$ | $\odot$ | $\odot$ | $2\times n$ | 0.6794748306274414 |

Our analysis shows that all recommended curves are vulnerable to SVA attack, unlike some like textbfsect163k1, sect233r1, sect409r1, K-163, B-233, B-409 which are resistant to ZVP attack. This shows how dangerous the attack is and raises questions about the effective security of the curves recommended by NIST and SECG

# 5. Conclusion

In this work, we analyzed the Same Values Analysis (SVA) side-channel attack on elliptic curves defined over binary fields, focusing on the Weierstrass, Edwards, and Hessian models. By systematically identifying conditions that lead to identical intermediate values during point addition and doubling, we demonstrated that collisions can be exploited to weaken scalar multiplication, the core operation of elliptic curve cryptography.

Our findings reveal that not only classical curves but also binary models recommended by NIST and SECG remain vulnerable to SVA attacks. This highlights an urgent need to reassess the trust placed in existing elliptic curve standards.

From a broader perspective, these results have important implications for cryptographic standardization. First, the criteria for curve selection in standards should explicitly include resistance to SVA and related algebraic side-channel attacks, beyond the traditional focus on discrete logarithm hardness. Second, secure parameter selection, such as avoiding curves or coordinate systems prone to repeated intermediate values should be a mandatory step in curve design. Finally, as the cryptographic community transitions toward post-quantum security, ensuring robustness of elliptic curves against advanced side-channel attacks remains a necessary requirement for hybrid schemes and legacy systems.

Future work should therefore combine algebraic analysis, implementation-level countermeasures, and post-quantum considerations to guide the next generation of secure elliptic curve standards.

## ORCID

0009-0007-2071-2645 (Aubain Jose Mayeukeu)
0000-0002-7729-0419 (Emmanuel Fouotsa)
0000-0002-0784-1377 (Celestin Lele)

## Abbreviations

| | |
|---|---|
| SVA | Same Value Analysis |
| ZVP | Zero Value Point |
| add | Addition of Points on Elliptic Curve |
| dbl | Doubling of Points on Elliptic Curve |
| SPA | Simple Power Analysis |
| DPA | Differential Power Analysis |
| RPA | Refined Power Analysis |
| NIST | National Institute of Standards and Technology |
| SECG | Standard for Efficient Cryptography Group |
| ECC | Elliptic Curve Cryptography |
| SCA | Side Channel Attack |
| WBDC | Weierstrass Binary Doubling Condition |
| WBAC | Weierstrass Binary Addition Condition |
| EBDC | Edwards Binary Doubling Condition |
| EBAC | Edwards Binary Addition Condition |
| HBDC | Hessian Binary Doubling Condition |
| HBAC | Hessian Binary Addition Condition |
| WPDC | Weierstrass Primary Doubling Condition |
| WPAC | Weierstrass Primary Addition Condition |

## Author Contributions

**Aubain Jose Mayeukeu:** Conceptualization, Formal Analysis, Methodology, Writing - original draft

**Emmanuel Fouotsa:** Conceptualization, Methodology, Supervision, Validation, Writing - review & editing

**Celestin Lele:** Supervision, Validation

## Conflicts of Interest

The authors declare no conflits of interest.

## References

[1] VS. Miller (1985) "Use of elliptic curves in cryptography". In: Springer. 1985: pp 417-426.

[2] N. Koblitz (1987) "Elliptic curve cryptosystems". In: Mathematics of computation. 1987;48(177) pp. 203-209.

[3] P. Kocher, J. Jaffe, B. Jun (1998) "Introduction to differential power analysis and related attacks" 1998.

[4] JS. Coron (1999) "Resistance against differential power analysis for elliptic curve cryptosystems" In: Springer. 1999, pp. 292-302.

[5] M. Joye, C. Tymen, "Protections against differential analysis for elliptic curve cryptography an algebraic approach". In: Springer. 2001, pp. 377-390.

[6] L. Goubin (2002) "A refined power-analysis attack on elliptic curve cryptosystems" In: Springer. 2002, pp. 199-211.

[7] NP. Smart, "An analysis of Goubin's refined power analysis attack" In: Springer. 2003, pp. 281-290.

[8] T. Akishita, T. Takagi, "Zero-value point attacks on elliptic curve cryptosystem" In: Springer. 2003, pp. 218-233.

[9] C. Crépeau, RA. Kazmi (2012). "An Analysis of ZVP-Attack on ECC Cryptosystems". Cryptology ePrint Archive. 2012.

[10] C. Murdica, S. Guilley, JL. Danger, P. Hoogvorst, D. Naccache (2012). "Same values power analysis using special points on elliptic curves" In: Springer. 2012, pp. 183-198.

[11] R. Abarzúa, S. Martínez, V. Mendoza, N. Thériault (2020) "Same value analysis on Edwards curves" In Journal of Cryptographic Engineering. 2020;10(1), pp. 27-48.

[12] A. Battistello, G. Bertoni, M. Corrias, L. Nava, D. Rusconi, M. Zoia, A. Lanzi (2025). "Unveiling ECC Vulnerabilities: LSTM Networks for Operation Recognition in Side-Channel Attacks". arXiv preprint arXiv:2502.17330, 2025.

[13] A. C. Canto, J. Kaur, M. Kermani, R. Azarderakhsh (2023). "Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security". arXiv preprint arXiv:2305.13544. 2023.

[14] Y. Ji, R. Wang, K. Ngo, E. Dubrova, L. Backlund (2023). "A side-channel attack on a hardware implementation of CRYSTALS-Kyber". In 2023 IEEE European Test Symposium (ETS). 2023, pp. 1-5.

[15] A. Shaller, L. Zamir, M. Nojoumian (2023). "Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures". Information and Computation, 295 , 105112. 2023.

[16] DJ. Bernstein (2007). "Explicit formulas database" http://www.hyperelliptic.org/EFD.2007

[17] J. López, R. Dahab (1999). "Fast multiplication on elliptic curves over GF (2m) without precomputation" In: Springer. 1999, pp. 316-327.

[18] RA. Kazmi, "Isogenies and cryptography" In: Cryptology ePrint Archive. 2010.

[19] AJ. Mayeukeu , E. Fouotsa (2024). "Same Values Analysis Attack on Weierstrass Binary Elliptic Curves" In: Springer. 2024, pp. 311-326.