Kummer and Hessian meet in the Field of Characteristic 2

Sabyasachi Karati[1] and Gourab Chandra Saha[2]

[1] Cryptology and Security Research Unit, Indian Statistical Institute, India
skarati@isical.ac.in
[2] Applied Statistics Unit, Indian Statistical Institute, India
gourab.chandra.saha@gmail.com

Abstract. One can compute scalar multiplication on an ordinary short Weierstrass curve defined over a binary field. Also, one can move to the associated binary Kummer line $\mathsf{BKL}_{(1:c)}$, or isomorphic generalized Hessian curve $\mathsf{H}_{(\gamma,\delta)}$ from short Weierstrass, and then compute the scalar multiplication. A generalized Hessian curve provides the best performance of scalar multiplication in $\mathfrak{RT}$ coordinates where $\mathfrak{R} = R^3+S^3$ and $\mathfrak{T} = T^3$ for a point $P = (R : S : T)$ on $\mathsf{H}_{(\gamma,\delta)}$. Montgomery scalar multiplication gives us the nP and $(n+1)P$, again in $\mathfrak{RT}$. We propose a method to uniquely obtain the R and S coordinates of nP given $P = (R : S : T)$ and $\mathfrak{RT}$ coordinates of nP and $(n+1)P$. Next, we show that $\mathsf{BKL}_{(1:c)}$ can be linked to an isomorphic $\mathsf{H}_{(\gamma,\delta)}$. But small c does not guarantee small γ or δ. First, we introduce two isogenies and their duals: one 2-isogeny between two short Weierstrass curves and one 3-isogeny between two generalized Hessian curves to solve the issue. Using the introduced isogenies, we show that there always exists a generalized Hessian curve $\mathsf{H}_{(\gamma,1)}$ with $\sqrt{\gamma^3(\gamma+1)} = c$ associated with a $\mathsf{BKL}_{(1:c)}$. The obtained $\mathsf{H}_{(\gamma,1)}$ needs $5[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}_s]$ field operations for each ladder step of Montgomery scalar multiplication, and the operation count is the smallest one compared to any other curves over a binary field.

Keywords: Binary Kummer line, Generalized Hessian curve, Scalar multiplication, Montgomery ladder, Isogeny.

1 Introduction

Elliptic curve cryptography was introduced by Miller [22] and Koblitz [20]. Elliptic curves are widely used to implement real-world public-key cryptographic primitives like Diffie-Hellman Key Exchange and Digital signatures [5] because elliptic curve provides small key sizes and signature sizes. Scalar multiplication is the basic building block of these protocols. We can categorize the scalar multiplications into two types: (i) Fixed-base scalar multiplication, where the point is known and fixed during the setup phase, and (ii) Variable-base scalar multiplication where the point is unknown beforehand. We need one fixed-base and one variable-base scalar multiplication for the Diffie-Hellman key exchange. On the other hand, key generation and signing of Elliptic Curve Digital Signature Algorithm (ECDSA) [12] each needs one fixed-base scalar multiplication, and

verification needs one fixed- and one variable-base scalar multiplication or a multi-scalar multiplication. Improvement in the performance of the scalar multiplication directly affects the computational time of these protocols, and secure and efficient scalar multiplication became a prerequisite for practical deployment.

To improve the performance of scalar multiplication, we must consider several aspects of the target application. First, assume that the underlying system does not support parallelization and possibly resource constraints. In this case, one should choose the form of the curve that takes the minimum number of field operations to perform the curve arithmetic. Second, consider that the underlying system has a parallelization feature. Now, we should choose the curve that provides the best-parallelized performance for the curve arithmetic. Third, the curve should have small curve parameters and a small base point so that the implementation can take advantage of optimized fixed-base scalar multiplication.

Over fields of large prime characteristic, it has been shown that Kummer line [19, 23] provides the best x-coordinate-based scalar multiplication if the Single-Instruction-Multiple-Data (SIMD) feature is available. For Diffie-Hellman key exchange, x-coordinate-based arithmetic is sufficient, and one can choose the Kummer Line. But if SIMD is unavailable, Montgomery curve $\mathsf{Curve25519}$ [1] should be chosen because it needs fewer field operations. On the other hand, one can take advantage of the twisted Edwards curve to have the best performance of digital signatures [13]. [18, 14] study the connections among these different forms of elliptic curves to facilitate more flexibility in the choice of the curves.

1.1 Our Contribution

In this work, we focus on finite fields of characteristics two. Kummer line $\mathsf{BKL}_{(1:c)}$ over the binary field was proposed by Gaudry and Lubicz [11]. The idea of scalar multiplication using the $\mathsf{BKL}_{(1:c)}$ was studied and [17] develops all the relevant details. $\mathsf{BKL}_{(1:c)}$ is defined by a projection map from a particular form of Weierstrass curve ($\mathsf{BEw}_{(c^4)} : y^2+xy = x^3+c^4$) to a projective line [11, 17]. The $\mathsf{BKL}_{(1:c)}$ provides the fastest x-coordinate-based scalar multiplication where parallelization is not available [17]. Hessian curve $\mathsf{H}_{(\delta)}$ was introduced by Smart [26], and [26] further shows that $\mathsf{H}_{(\delta)}$ is suitable for parallelization. Farashahi and Joye proposed the concept of a Generalized Hessian curve $\mathsf{H}_{(\gamma,\delta)}$ [7], and the $\mathsf{H}_{(\delta)}$ becomes a special case with $\gamma = 1$. The twisted Hessian curve $\mathsf{H}^t_{(\rho,\delta)}$ was proposed by Bernstein, Chuengsatiansup, Kohel, and Lange [3], and it is isomorphic to a generalized Hessian curve $\mathsf{H}_{(\gamma,\delta)}$. The generalized Hessian curve provides *unified* formulas of curve arithmetic and has been shown that the formulas are more efficient when the underlying field is of characteristic two.

Field square is significantly faster than field multiplication over a finite field of characteristic 2. Thus, $\mathsf{BKL}_{(1:c)}$ ($5[\mathsf{M}]+5[\mathsf{S}]+1[\mathsf{C}_s]$ per bit of scalar[3]) provides faster scalar multiplication than $\mathsf{H}_{(\gamma,\delta)}$ ($6[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}_s]$ per bit of scalar) if the underlying platform does not support parallelization. On the other hand,

[3] $\mathsf{M}, \mathsf{S}, \mathsf{C}$, and C_s denotes a field multiplication, a square, a multiplication by a constant, and a multiplication by a small constant.

[26, 7] show that $\mathsf{H}_{(\gamma,\delta)}$ is efficiently parallelizable, but effect of parallelization on $\mathsf{BKL}_{(1:c)}$ is not known. In this work, we show the connection between $\mathsf{BKL}_{(1:c)}$ and $\mathsf{H}_{(\gamma,\delta)}$ via isomorphism that supports interoperability between different platforms so that platforms with SIMD feature can take advantage of $\mathsf{H}_{(\gamma,\delta)}$ while platforms without SIMD feature can take advantage of $\mathsf{BKL}_{(1:c)}$. We also show that we can connect $\mathsf{BKL}_{(1:c)}$ to a $\mathsf{H}_{(\gamma,1)}$, via isogeny, that supports faster scalar multiplication ($5[\mathsf{M}]+4[\mathsf{S}]+1[\mathsf{C}_s]$ per bit of scalar) than the associated $\mathsf{BKL}_{(1:c)}$ on platforms without SIMD feature. Therefore, one can take advantage of scalar multiplication of the Kummer line by moving from $\mathsf{BEw}_{(c^4)}$ to the Kummer Line $\mathsf{BKL}_{(1:c)}$ or generalized Hessian curve by moving to $\mathsf{H}_{(\gamma,\delta)}$. A brief description of our contributions is given below.

1. **Retrieve R and S-coordinates of generalized Hessian curve in $\mathfrak{RT}$ coordinate system.** To achieve the best possible operation count per bit of the scalar for x-coordinate-based scalar multiplication, a binary Kummer line uses **xz** coordinates and a generalized Hessian uses $\mathfrak{RT}$-coordinates where $\mathfrak{R} = R^3+S^3$ and $\mathfrak{T} = T^3$ for a point $P = (R : S : T)$ on a generalized Hessian curve. Using $\mathfrak{RT}$ coordinates with Montgomery scalar multiplication, one computes two points $nP = (R_n : S_n : T_n)$ and $(n+1)P = (R_{n+1} : S_{n+1} : T_{n+1})$, but they are again in $\mathfrak{RT}$ coordinate. Recovering R_n and S_n is an important problem but no solution is available in the literature. We propose a method for the first time that allows us to compute unique R_n and S_n from the known details $R, S, T, R_n^3 + S_n^3, T_n^3$, $R_{n+1}^3 + S_{n+1}^3$, and T_{n+1}^3.
2. **Connecting Binary Kummer/Weierstrass to Binary Hessian using Isomorphism.** One can choose a generalized Hessian curve for scalar multiplication. [7] shows that there exists an isomorphic generalized Hessian curve if the Weierstrass curve has a point of order three and provides the corresponding mapping. But one particular map is not isomorphic. We give the explicit map for binary fields following the map given in [30], and we connect binary Kummer line $\mathsf{BKL}_{(1:\sqrt[4]{c})}$ by connecting short Weierstrass curve $\mathsf{BEw}_{(c)}$ to a generalized Hessian curve. The obtained isomorphic generalized Hessian curve needs $5[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}] + 1[\mathsf{C}_s]$ field operations and for large constant it becomes $6[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}_s]$.
3. **Connecting Binary Kummer/Weierstrass to Binary Hessian using Isogeny.** First, we propose two isogenies and their duals: (i) ϕ is a 2-isogeny between the short Weierstrass curves $\mathsf{BEw}_{(b)}$ and $\mathsf{BEw}_{(\sqrt{b})}$, and (ii) ξ is a 3-isogeny between generalized Hessian curves $\mathsf{H}_{(a^3,1)}$ and $\mathsf{H}_{(\gamma,1)}$ with $\gamma = a + a^2 + a^3$. Next, with the help of ϕ and ξ, we connect binary Kummer line $\mathsf{BKL}_{(1:c)}$ by showing that a short Weierstrass curve $\mathsf{BEw}_{(c^4)}$ is isogenous to the generalized Hessian curve $\mathsf{H}_{(x_3,1)}$ where (x_3, y_3) is a point of order 3 on $\mathsf{BEw}_{(c^2)}$. The $\mathsf{H}_{(x_3,1)}$ requires $5[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}_s]$ field operations for the arithmetic of each ladder step of Montgomery scalar multiplication which is the smallest one for variable-base scalar multiplication compared to the present state-of-the-art over binary fields as given in Table 1.
4. We go beyond the task of just providing the mappings and optimized arithmetic on the generalized Hessian Curve and propose concrete Kummer lines

Table 1. Comparison of operation counts per ladder step for variable base scalar multiplication over different curves

Curve	Coordinates	Operation Count per Ladder Step
Short Weirstrass Curve [27]	XZ	$5[\mathsf{M}] + 6[\mathsf{S}] + 2[\mathsf{C}_s]$
Binary Kummer line [17]	$\mathbf{xz}$	$5[\mathsf{M}] + 5[\mathsf{S}] + 1[\mathsf{C}_s]$
Binary Edwards Curve [17]	$\mathfrak{U}W$	$5[\mathsf{M}] + 4[\mathsf{S}] + 2[\mathsf{C}_s]$
Generalized Hessian Curve [7]	$\mathfrak{RT}$	$5[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}] + 1[\mathsf{C}_s]$
Generalized Hessian Curve (this work)	$\mathfrak{RT}$	$\mathbf{5}[\mathsf{M}] + \mathbf{4}[\mathsf{S}] + \mathbf{1}[\mathsf{C_s}]$

with small curve parameters and associated binary generalized Hessian curves, and binary Hessian curves with small curve parameters and the associated binary Kummer lines.

2 Background

This section includes brief descriptions of the relevant curves: short Weierstrass curve, binary Kummer Line, and generalized Hessian curve over $\mathbb{F}_{2^m}$ where $\mathbb{F}_{2^m}$ denotes a finite field of characteristic two with 2^m elements for some $m \in \mathbb{N}$.

2.1 Weierstrass Curve

A short Weierstrass affine form of a non-supersingular elliptic curve over $\mathbb{F}_{2^m}$ is given by the Equation (1) [12]:

$$\mathsf{BEw}_{(a,b)}: \quad y^2 + xy = x^3 + ax^2 + b, \tag{1}$$

where $b \neq 0$. All the points (x, y) of the affine plane $\mathbb{A}^2 = \mathbb{F}_{2^m}^2$ that satisfy the equation of the curve $\mathsf{BEw}_{(a,b)}$ along with a special point $\mathcal{O}$, called point at infinity, form an additive group. The projective form of a short Weierstrass curve is given by the Equation (2):

$$\mathsf{BEw}_{(a,b)}: \quad Y^2 + XYZ = X^3 + aX^2Z + bZ^3. \tag{2}$$

The affine point (x, y) can be identified with the projective points $(X : Y : Z) \in \mathbb{P}^2 = \mathbb{F}_{2^m}^3 \setminus \{0 : 0 : 0\}$ where $x = X/Z$ and $y = Y/Z$. We say two projective points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are called equivalent if there exists a non-zero $\lambda \in \mathbb{F}_{2^m}$ such that $X_1 = \lambda X_2$, $Y_1 = \lambda Y_2$ and $Z_1 = \lambda Z_2$. The point at infinity $\mathcal{O}$ is the equivalent class of points with $Z = 0$. In the article, we will use the projective versions mainly because of their practical relevance. But sometimes we use the affine version in proofs for simplicity.

2.2 Binary Kummer Line

In this work, we are specifically interested in short Weierstrass curve $\mathsf{BEw}_{(a,b)}$ with $a = 0$ and we denote it by $\mathsf{BEw}_{(b)}$ whose projective form is given by Equation (3):

$$\mathsf{BEw}_{(b)}: \quad Y^2Z + XYZ = X^3 + bZ^3. \tag{3}$$

Let $c \in \mathbb{F}_{2^m}$ and $c \neq 0$. A binary Kummer line $\mathsf{BKL}_{(1:c)}$ is defined over projective space $\mathbb{P}^1$ by mapping $\pi : \mathsf{BEw}_{(c^4)}/\{\pm 1\} \to \mathsf{BKL}_{(1:c)}$ [17, 11] as:

$$\pi(P = (X : \cdot : Z)) = \begin{cases} (cZ : X), \text{ if } X \neq 0 \\ (0 : 1), \text{ if } X = 0. \end{cases} \tag{4}$$

For each $c \in \mathbb{F}_{2^m}$, $\mathsf{BEw}_{(c)}$ has a unique $\mathsf{BKL}_{(1:\sqrt[4]{c})}$ because each c has a unique square-root in a binary field.

[11] derives the arithmetic of binary Kummer line over projective space $\mathbb{P}^1$ using theta functions. Each point of $\mathsf{BKL}_{(1:c)}$ in $\mathbb{P}^1$ is defined as $(\mathbf{x}, \mathbf{z}) \in \mathbb{F}_{2^m}^2$. Two points $\mathbf{P} = (\mathbf{x}_1, \mathbf{z}_1)$ and $\mathbf{Q} = (\mathbf{x}_2, \mathbf{z}_2)$ are said to be equivalent if there exists a non-zero $\lambda \in k$ such that $\mathbf{x}_1 = \lambda \mathbf{x}_2$ and $\mathbf{z}_1 = \lambda \mathbf{z}_2$. Let $\mathbf{P} = (\mathbf{x}_1, \mathbf{z}_1)$ and $\mathbf{Q} = (\mathbf{x}_2, \mathbf{z}_2)$ be two points on $\mathsf{BKL}_{(1:c)}$ with known $\mathbf{P} - \mathbf{Q} = (\mathbf{x}, \mathbf{z})$. By Doubling Algorithm $\mathtt{dbl}_k$ and Differential Addition Algorithm $\mathtt{diffAdd}_k$ of Table 2, we compute $2\mathbf{P} = (\mathbf{x}_3, \mathbf{z}_3)$ and $\mathbf{P} + \mathbf{Q} = (\mathbf{x}_4, \mathbf{z}_4)$, respectively. In $\mathsf{BKL}_{(1:c)}$, $\mathbf{I} = (1, 0)$ is an identity and the point $(0, 1)$ is a point of order two [17]. With $\mathbf{z} = 1$, we need $5[\mathsf{M}] + 5[\mathsf{S}] + 1[\mathsf{C}_s]$ to compute $\mathtt{dbl}_k$ and $\mathtt{diffAdd}_k$ in total.

Table 2. Doubling and Differential Addition on Binary Kummer line

$(\mathbf{x}_3, \mathbf{z}_3) = \mathtt{dbl}_k(\mathbf{x}_1, \mathbf{z}_1)$:	$(\mathbf{x}_4, \mathbf{z}_4) = \mathtt{diffAdd}_k(\mathbf{x}_1, \mathbf{z}_1, \mathbf{x}_2, \mathbf{z}_2, \mathbf{x}, \mathbf{z})$:
$\mathbf{x}_3 = c(\mathbf{x}_1^2 + \mathbf{z}_1^2)^2$;	$\mathbf{x}_4 = \mathbf{z}(\mathbf{x}_1\mathbf{x}_2 + \mathbf{z}_1\mathbf{z}_2)^2$;
$\mathbf{z}_3 = (\mathbf{x}_1\mathbf{z}_1)^2$;	$\mathbf{z}_4 = \mathbf{x}(\mathbf{x}_1\mathbf{z}_2 + \mathbf{x}_2\mathbf{z}_1)^2$;

The inverse mapping $\pi^{-1} : \mathsf{BKL}_{(1:c)} \to \mathsf{BEw}_{(c^4)}/\{\pm 1\}$ maps a point $\mathbf{P}$ of Kummer line $\mathsf{BKL}_{(1:c)}$ to elliptic curve $\mathsf{BEw}_{(c^4)}$ as given by Equation (5) [11]:

$$\pi^{-1}(\mathbf{P} = (\mathbf{x} : \mathbf{z})) = \begin{cases} (c\mathbf{z} : \cdot : \mathbf{x}), \text{ if } \mathbf{x} \neq 0 \\ \mathcal{O}, \text{ if } \mathbf{x} = 0. \end{cases} \tag{5}$$

Notice that the points on $\mathsf{BEw}_{(c^4)}$ are in $\mathbb{P}^2$. Putting $x = \frac{c\mathbf{z}}{\mathbf{x}}$ in Equation (3), we can compute the Y-coordinate up to elliptic involution.

But the mapping π alone does not conserve the consistency of the scalar multiplications between Kummer line $\mathsf{BKL}_{(1:c)}$ and the elliptic curve $\mathsf{BEw}_{(c^4)}$. [17] extends the mapping π to $\hat{\pi}$ with the help of the point of order two $T_2 = (0, c^2)$ on $\mathsf{BEw}_{(c^4)}$. Definitions of $\hat{\pi}$ and $\hat{\pi}^{-1}$ are given in Equation (6).

$$\hat{\pi}(P) = \pi(P + T_2); \text{ and } \hat{\pi}^{-1}(\mathbf{P}) = \pi^{-1}(\mathbf{P}) + T_2. \tag{6}$$

2.3 Binary Generalized Hessian Curve

Hessian curve was introduced by Smart [26], and Joye and Quisquater [16] in 2001. Hessian curve was proposed to achieve side-channel resistant elliptic curve cryptography. Smart [26] also showed that it achieves significant speedups using parallelization. Farashahi and Joye developed the concept of Generalized Hessian Curves in 2010 [7].

Let $\mathbb{F}_{2^m}$ be a finite field, and let $\gamma, \delta \in \mathbb{F}_{2^m}$ such that $\gamma, \delta \neq 0$ and $\delta^3 \neq \gamma$. The projective form of Generalized Hessian Curve [7] is defined by

$$\mathsf{H}_{(\gamma,\delta)} : R^3 + S^3 + \gamma T^3 = \delta RST \tag{7}$$

The identity element of $\mathsf{H}_{(\gamma,\delta)}$ is $(1:1:0)$ and it is denoted by $\mathcal{O}_H$. If $P = (R : S : T)$ be a point on $\mathsf{H}_{(\gamma,\delta)}$, then $-P = (S : R : T)$.

Let $P_1 = (R_1 : S_1 : T_1)$ and $P_2 = (R_2 : S_2 : T_2)$ be two points on $\mathsf{H}_{(\gamma,\delta)}$. In $\mathfrak{R}\mathfrak{T}$ coordinate system, the points are $P_1 = (\mathfrak{R}_1 : \mathfrak{T}_1) = (R_1^3 + S_1^3 : T_1^3)$ and $P_2 = (\mathfrak{R}_2 : \mathfrak{T}_2) = (R_2^3 + S_2^3 : T_2^3)$. Let $P = P_2 - P_1 = (\mathfrak{R} : 1)$ is given to us. Note that, in $\mathfrak{R}\mathfrak{T}$ coordinates, $P_1 - P_2 = P_2 - P_1 = (R^3 + S^3 : 1) = (\mathfrak{R} : 1)$. Now we compute $P_3 = 2P_1 = (\mathfrak{R}_3 : \mathfrak{T}_3)$ and $P_4 = P_1 + P_2 = (\mathfrak{R}_4 : \mathfrak{T}_4)$ by $(P_3, P_4) = \mathsf{m\_dbl\_diffAdd}(P_1, P_2, P)$ given in Table 3 and needs $5[\mathsf{M}]+4[\mathsf{S}]+3[\mathsf{C}]$.

Table 3. Mixed Doubling and Differential Addition ($\mathsf{m\_dbl\_diffAdd}$) on $\mathsf{H}_{(\gamma,\delta)}$

$A = \mathfrak{R}_1 * \mathfrak{T}_2, B = \mathfrak{R}_2 * \mathfrak{T}_1, C = A * B, D = \mathfrak{R}_1^2, E = \mathfrak{T}_1^2, F = D + \sqrt{\gamma^3(\delta^3+\gamma)}E,$ $G = \delta^3 C, H = \delta^3 E, \mathfrak{R}_3 = F^2, \mathfrak{T}_3 = D * H, \mathfrak{T}_4 = (A+B)^2, \mathfrak{R}_4 = G + \mathfrak{R} * \mathfrak{T}_4.$

Hessian Curve of [26, 16], denoted by H_δ, is a special form of the Generalized Hessian Curve $\mathsf{H}_{(\gamma,\delta)}$ with $\gamma = 1$ and is defined as $\mathsf{H}_{(\delta)} : R^3 + S^3 + T^3 = \delta RST$. Let $\mathbb{F}_{2^m}\left(\sqrt[3]{\gamma}\right)$ be the smallest extension field containing $\mathbb{F}_{2^m}$ and $\sqrt[3]{\gamma}$. Now we define the map

$$\begin{aligned} \varphi : \mathsf{H}_{(\gamma,\delta)} &\longrightarrow \mathsf{H}_{(\delta/\sqrt[3]{\gamma})} \\ (R : S : T) &\mapsto (R : S : \sqrt[3]{\gamma}T) \end{aligned} \tag{8}$$

The mapping φ is an isomorphism from $\mathsf{H}_{(\gamma,\delta)}$ to $\mathsf{H}_{(\delta/\sqrt[3]{\gamma})}$ over $\mathbb{F}_{2^m}\left(\sqrt[3]{\gamma}\right)$. For $\mathsf{H}_{(\delta)}$, the total cost for a mixed differential addition and doubling is $5[\mathsf{M}]+4[\mathsf{S}]+2[\mathsf{C}]$ field operations. Now, by choosing small δ, one can make δ^3 small, but $\frac{1}{\delta^3}$ may not be a small constant, and the total cost becomes $5[\mathsf{M}]+4[\mathsf{S}]+1[\mathsf{C}]+1[\mathsf{C}_s]$ field operations (Table 4).

3 Retrieving the R and S-coordinates of nP

One of the objectives of this work is to have efficient scalar multiplication either via binary Kummer Line or via generlized Hessian curve. To have resistance

Table 4. Mixed Doubling and Differential Addition ($\mathsf{m\_dbl\_diffAdd}$) on $\mathsf{H}_{(\delta)}$

$A = \mathfrak{R}_1 * \mathfrak{T}_2, B = \mathfrak{R}_2 * \mathfrak{T}_1, C = A * B, D = \mathfrak{R}_1^2, E = \mathfrak{T}_1^2, F = D + E, G = \delta^3 C, H = \frac{1}{\delta^3} F,$ $\mathfrak{R}_3 = (E+H)^2, \mathfrak{T}_3 = D * E, \mathfrak{T}_4 = (A+B)^2, \mathfrak{R}_4 = G + \mathfrak{R} * \mathfrak{T}_4.$

against side-channel attacks like Timing attacks, Power attacks, Montgomery scalar multiplication is the most popular choice. Montgomery scalar multiplication is an x-coordinate-only scalar multiplication that enables us to achieve constant time scalar multiplication. Montgomery scalar multiplication is also used when resources are limited. In this section, we provide a brief description of Montgomery scalar multiplication. Montgomery ladder-based scalar multiplication achieves the best result in the **xz**-coordinate for binary Kummer line [17], XZ-coordinate for short Weierstrass [27] and $\mathfrak{RT}$ for generalized Hessian [7].

Let $P = (R : S : T)$ be a point on the generalized Hessian curve $\mathsf{H}_{(\gamma,\delta)}$. Then $P = (\mathfrak{R}, \mathfrak{T})$ with $\mathfrak{R} = R^3 + S^3$ and $\mathfrak{T} = T^3$ in $\mathfrak{RT}$ coordinates. We can compute $2P = (\mathfrak{R}_3, \mathfrak{T}_3) = \mathsf{dbl}_H(P)$ as given in [7, Equation 18]. Let $n = \{1, n_{l-2}, \ldots, n_1, n_0\}_2$ be an l-bit long scalar. We can compute $nP = (\mathfrak{R}_n, \mathfrak{T}_n)$ by Montgomery scalar multiplication as given in Table 5. We need one $\mathsf{m\_dbl\_diffAdd}$ for each bit of the scalar. After the i-th iteration, we have $\mathfrak{R}$- and $\mathfrak{T}$-coordinates of n_iP and $(n_i+1)P$ where $n_i = \{1, n_{l-2}, \ldots, n_i\}_2$. Montgomery ladder scalar multiplication always preserves the invariance $P = (n_i+1)P - n_iP$.

Table 5. Montgomery Ladder Scalar Multiplication

nP=scalarMult(P, n) :	ladderStep(P_1, P_2, n_i) :
1. Let $n = \{1, n_{l-2}, \ldots, n_0\}$;	1. If $n_i = 0$ then
2. $P_1 = P, R = \mathsf{dbl}_H(P)$;	2. $(P_1, P_2) = \mathsf{m\_dbl\_diffAdd}(P_1, P_2, P)$;
3. For $i = l-2$ to 0 do	3. Else If $n_i = 1$ then
4. laddarStep(P_1, P_2, n_i)	4. $(P_2, P_1) = \mathsf{m\_dbl\_diffAdd}(P_2, P_1, P)$;
5. End For;	5. End If
6. Return P_1;	

At the end of the ladder step, we have $nP = (\mathfrak{R}_n : \mathfrak{T}_n)$ and $(n+1)P = (\mathfrak{R}_{n+1} : \mathfrak{T}_{n+1})$ from the P and n in $\mathfrak{RT}$ coordinate system. Let $nP = (R_n : S_n : T_n)$ and $(n+1)P = (R_{n+1} : S_{n+1} : T_{n+1})$, then $\mathfrak{R}_n = R_n^3 + S_n^3$, $\mathfrak{T}_n = T_n^3$, $\mathfrak{R}_{n+1} = R_{n+1}^3 + S_{n+1}^3$ and $\mathfrak{T}_{n+1} = T_{n+1}^3$. Our objective is to retrieve the R_n and S_n explicitly from the known quantities R, S, T, $\mathfrak{R}_n$,$\mathfrak{T}_n$, $\mathfrak{R}_{n+1}$ and $\mathfrak{T}_{n+1}$. We use the affine coordinates for simplicity, and our problem reduces to computation of (r_n, s_n) explicitly given $r = R/T$, $s = S/T$, $\mathfrak{r}_n = \mathfrak{R}_n/\mathfrak{T}_n$, and $\mathfrak{r}_{n+1} = \mathfrak{R}_{n+1}/\mathfrak{T}_{n+1}$.

Let the underlying field be $\mathbb{F}_{2^m}$ for some $m \in \mathbb{N}$. During retrieval of (r_n, s_n), we show that there will be two points (if m is odd) or six points (if m is even) if $\mathfrak{r}_n = \mathfrak{r} = r^3 + s^3$ on the curve which satisfy that $(n+1)P = nP + P$ and $\mathfrak{r}_n = r_n^3 + s_n^3$. Therefore, we need $\mathfrak{r}_n$ *must not be the same as* $\mathfrak{r}$. Theorem 2 shows how we should choose the P and the scalar n to have $\mathfrak{r}_n \neq \mathfrak{r}$. The proof of Theorem 2 uses Lemmas 1 and 2, and Theorem 1. This also shows that we can always explicitly compute (r_n, s_n) for the generalized Hessian curves used in cryptography.

Lemma 1. *Let* $\mathsf{H}_{(\gamma,\delta)} : r^3 + s^3 + \gamma = \delta rs$ *be a generalized Hessian curve in affine coordinate over* $\mathbb{F}_{2^m}$*. Then, there exists a point of* (r, s) *on* $\mathsf{H}_{(\gamma,\delta)}$ *satisfying* $r^3 + s^3 = \mathfrak{r}$ *if and only if*

1. $\mathrm{Tr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) = 0$*, and*
2. *If* m *is even, then* β *has cube roots in* $\mathbb{F}_{2^m}$*, where* $\beta = \mathfrak{r}\sum_{i=0}^{m-2}\left(\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)^{2^i}\sum_{j=i+1}^{m-1}\mu^{2^j}\right)$ *and* $\mu \in \mathbb{F}_{2^m}$ *with* $\mathrm{Tr}(\mu) = 1$.

Proof. Let $\mathrm{Tr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) = 0$. It is equivalent to saying that there exists a non-zero $r' \in \mathbb{F}_{2^m}$ such that $r'^2 + \mathfrak{r}r' + \frac{(\gamma+\mathfrak{r})^3}{\delta^3} = 0$. Now we can rewrite the equation as $r' + \mathfrak{r} + \frac{(\gamma+\mathfrak{r})^3}{r'\delta^3} = 0 \iff r' + \frac{(\gamma+\mathfrak{r})^3}{r'\delta^3} = \mathfrak{r} \iff r' + s' = \mathfrak{r}$, where $s' = \frac{(\gamma+\mathfrak{r})^3}{r'\delta^3}$. If r' is a cube in $\mathbb{F}_{2^m}$ and let $r^3 = r'$, then we have $s' = \left(\frac{(\gamma+\mathfrak{r})^3}{r^3\delta^3}\right) = s^3$ with $s = \frac{\gamma+\mathfrak{r}}{r\delta}$. As a consequence, we get $\gamma + \delta rs = \mathfrak{r} = r' + s' = r^3 + s^3$, that is $r^3 + s^3 + \gamma = \delta rs$.

If m is odd, then roots of the equation $r'^2 + \mathfrak{r}r' + \left(\frac{(\gamma+\mathfrak{r})^3}{\delta^3}\right) = 0$ are $\mathfrak{r} \times \mathsf{HTr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)$ and $\left(\mathfrak{r} \times \mathsf{HTr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) + \mathfrak{r}\right)$ [4]. Also, odd m ensures that every element of $\mathbb{F}_{2^m}$ has a unique cube root, and so do r' and s'. Therefore, (r, s) is a point on the curve $\mathsf{H}_{(\gamma,\delta)}$ such that $r^3 + s^3 = \mathfrak{r}$.

If m is even, then the roots of the equation $r'^2 + \mathfrak{r}r' + \left(\frac{(\gamma+\mathfrak{r})^3}{\delta^3}\right) = 0$ are β and $\beta + \mathfrak{r}$, where $\beta = \mathfrak{r}\sum_{i=0}^{m-2}\left(\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)^{2^i}\sum_{j=i+1}^{m-1}\mu^{2^j}\right)$ and $\mu \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}(\mu) = 1$ [4]. Let $r' = \beta$, and if β is a cube, then there exists a $r \in \mathbb{F}_{2^m}$ such that $r^3 = r' = \beta$. Therefore $s = \frac{\gamma+\mathfrak{r}}{r\delta} \in \mathbb{F}_{2^m}$. Now we have $s^3 = r^3 + \mathfrak{r} = \beta + \mathfrak{r}$. Therefore, $\beta + \mathfrak{r}$ also be a cube, and there is a point (r, s) on the curve $\mathsf{H}_{(\gamma,\delta)}$ with $r^3 + s^3 = \mathfrak{r}$.

The other direction is trivially true. □

Lemma 2. *Let* $\mathsf{H}_{(\gamma,\delta)} : r^3 + s^3 + \gamma = \delta rs$ *be a generalized Hessian curve over* $\mathbb{F}_{2^m}$*. Let there be points* (r, s) *on* $\mathsf{H}_{(\gamma,\delta)}$ *such that* $r^3 + s^3 = \mathfrak{r}$*. If* m *is odd, then there are two such points, else there are six such points.*

Proof. 1. Let m be odd. If $r^3 + s^3 = \mathfrak{r}$, the equation $r'^2 + \mathfrak{r}r' + \left(\frac{(\gamma+\mathfrak{r})^3}{\delta^3}\right) = 0$ has roots in $\mathbb{F}_{2^m}$ by Lemma 1 as $\mathrm{Tr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) = 0$. The roots are $\mathfrak{r}\lambda_1$ and $\mathfrak{r}\lambda_1 + \mathfrak{r}$

where $\lambda_1 = \mathsf{HTr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)$. Again, each element of $\mathbb{F}_{2^m}$ has a unique root in $\mathbb{F}_{2^m}$ if m is odd. Therefore, there exists $r_1, r_2 \in \mathbb{F}_{2^m}$ such that $r_1^3 = \mathfrak{r}\lambda_1$ and $r_2^3 = \mathfrak{r}\lambda_1 + \mathfrak{r}$. For each $r_i, i = 1, 2$, there is a unique $s_i = \frac{\gamma+\mathfrak{r}}{r_i\delta}$. Then there are two points $(r_i, s_i), i = 1, 2$ on $\mathsf{H}_{(\gamma,\delta)}$ such that $r_i^3 + s_i^3 = \mathfrak{r}$.

2. If m is even, then the roots of the equation $r'^2 + \mathfrak{r}r' + \left(\frac{(\gamma+\mathfrak{r})^3}{\delta^3}\right) = 0$ are $\mathfrak{r}\lambda_2$ and $\mathfrak{r}\lambda_2 + \mathfrak{r}$ where $\lambda_2 = \sum_{i=0}^{m-2}\left(\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)^{2^i}\sum_{j=i+1}^{m-1}\mu^{2^j}\right)$ as $\mathrm{Tr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) = 0$ from Lemma 1. Let the roots be $r_1^3 = \mathfrak{r}\lambda_2$ and $r_2^3 = \mathfrak{r}\lambda_2 + \mathfrak{r}$. If $r_1^3 = \mathfrak{r}\lambda_2$ has a solution in $\mathbb{F}_{2^m}$, then it has three roots as $r_1, r_1\omega$ and $r_1\omega^2$ where ω is a primitive cube root of unity in $\mathbb{F}_{2^m}$. For each such cube root, we have a point $(r_1\omega^i, s_{1,i})$ with $s_{1,i} = \frac{\gamma+\mathfrak{r}}{r_1\omega^i\delta}$ for $i = 0, 1, 2$ on $\mathsf{H}_{(\gamma,\delta)}$ such that $r_1^3\omega^{3i} + s_{1,i}^3 = \mathfrak{r}$. In Lemma 1, we have shown that if there are solutions of $r_1^3 = \mathfrak{r}\lambda_2$, there are solutions for $r_2^3 = \mathfrak{r}\lambda_2 + \mathfrak{r}$. Similarly, we get another three such points $(r_2\omega^i, s_{2,i})$ where $r_2^3\omega^{3i} + s_{2,i}^3 = \mathfrak{r}$. Therefore, we have six points (r, s) on $\mathsf{H}_{(\gamma,\delta)}$ such that $r^3 + s^3 = \mathfrak{r}$. □

Theorem 1. *Let $\mathsf{H}_{(\gamma,\delta)} : r^3 + s^3 + \gamma = \delta rs$ be a generalized Hessian curve over $\mathbb{F}_{2^m}$. Let P and Q be two points on the curve with $r^3 + s^3 = \mathfrak{r}$. Then $Q - P$ is a point of order 3, or the point $2Q$, or $2Q + P_3$, where P_3 is a point of order three.*

Proof. We prove the theorem in two parts. First, we proof for $\mathbb{F}_{2^m}$ for some odd m, and then for even m.

– **Let m be odd.** From Lemma 1, we have two points (r_i, s_i) with $r_i^3 = \mathfrak{r} \times \mathsf{HTr}\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right) + \mathfrak{r} \times (i-1)$ and $s_i = \frac{\gamma+1}{r_i\delta}$ for $i = 1, 2$ such that $r_i^3 + s_i^3 = \mathfrak{r}$. Let $P = (r_1, s_1)$ and $Q = (r_2, s_2)$, then $r_1^3 r_2^3 = \left(\frac{\gamma+\mathfrak{r}}{\delta}\right)^3$, that is $r_1 r_2 = \frac{\gamma+\mathfrak{r}}{\delta}$. Using Equation (5) of [7], we get

$$\begin{aligned} P + Q &= (r_1 : s_1 : 1) + (r_2 : s_2 : 1) = \left(r_1 : \frac{\gamma+\mathfrak{r}}{r_1\delta} : 1\right) + \left(r_2 : \frac{\gamma+\mathfrak{r}}{r_2\delta} : 1\right) \\ &= ((\gamma+\mathfrak{r}) : r_2 r_1 \delta : 0) = ((\gamma+\mathfrak{r}) : (\gamma+\mathfrak{r}) : 0), \text{ where } r_1 r_2 = \frac{\gamma+\mathfrak{r}}{\delta} \\ &= (1 : 1 : 0). \end{aligned}$$

This implies that $P = -Q$. Therefore, $Q - P = 2Q$.

– **Let m be even.** Here $r_1^3 r_2^3 = \left(\frac{\gamma+\mathfrak{r}}{\delta}\right)^3$ and choose r_1, r_2 such that $r_1 r_2 = \frac{\gamma+\mathfrak{r}}{\delta}$. From Lemma 2, we have six points $(r_{i,j}, s_{i,j})$ with $r_{i,j} = r_i\omega^j$, $r_i^3 = \mathfrak{r} \times \sum_{k=0}^{m-2}\left(\left(\frac{(\gamma+\mathfrak{r})^3}{\mathfrak{r}^2\delta^3}\right)^{2^k}\sum_{j=k+1}^{m-1}\mu^{2^j}\right) + \mathfrak{r} \times (i-1)$ and $s_{i,j} = \frac{\gamma+\mathfrak{r}}{r_{i,j}\delta}$ for all $i = 1, 2$ and $j = 0, 1, 2$ such that $r_{i,j}^3 + s_{i,j}^3 = \mathfrak{r}$. Let $P = (r_{i,j}, s_{i,j})$ and $Q = (r_{i',j'}, s_{i',j'})$ and $(i, j) \neq (i', j')$. Now we compute $Q - P$ using the projective addition formulas given in [7] in three different situations.

1. Let $i = i'$, $j \neq j'$, and $j' = j + j''$ with $|j''| \in \{1, 2\}$. Using Equation (10) of [7] and $1/\omega^2 = \omega^3/\omega^2 = \omega$, we get

$$Q - P = (r_{i,j'} : s_{i,j'} : 1) - (r_{i,j} : s_{i,j} : 1) = \left(r_i\omega^{j'} : \frac{\gamma + \mathfrak{r}}{r_i\omega^{j'}\delta} : 1\right) - \left(r_i\omega^{j} : \frac{\gamma + \mathfrak{r}}{r_i\omega^{j}\delta} : 1\right)$$
$$= \left(\gamma r_i\omega^j + \frac{\omega^j(\gamma + \mathfrak{r})^3}{r_i^2\delta^3} : \gamma r_i\omega^{j+j''} + \frac{\omega^{j+j''}(\gamma + \mathfrak{r})^3}{r_i^2\delta^3} : 0\right) = (1 : \omega^{j''} : 0),$$

   which is a point of order 3.
2. Let $i \neq i'$ and $j + j' \equiv 0 \pmod 3$. Now we add the points using the projective addition formula given in Equation (5) of [7], we get

$$P + Q = (r_{i,j} : s_{i,j} : 1) + (r_{i',j'} : s_{i',j'} : 1) = \left(r_{i,j} : \frac{\gamma + \mathfrak{r}}{r_{i,j}\delta} : 1\right) + \left(r_{i',j'} : \frac{\gamma + \mathfrak{r}}{r_{i',j'}\delta} : 1\right)$$
$$= ((\gamma + \mathfrak{r}) : (\gamma + \mathfrak{r}) : 0), \text{ applying } r_{i,j}r_{i',j'} = r_ir_{i'}\omega^{j+j'} = \frac{\gamma + \mathfrak{r}}{\delta}$$
$$= (1 : 1 : 0),$$

   Hence, $P = -Q$ that implies $Q - P = 2Q$.
3. Let $i \neq i'$ and $j + j' \not\equiv 0 \pmod 3$. Then

$$Q - P = (r_{i',j'}, s_{i',j'}) - (r_{i,j}, s_{i,j}) = (r_{i',j'}, s_{i',j'}) - ((r_{i,-j' \pmod 3)}, s_{i,-j' \pmod 3)}) - P_3),$$
$$\text{where } P_3 \text{ be a point of order 3 by case 1}$$
$$= 2(r_{i',j'}, s_{i',j'}) + P_3 = 2Q + P_3, \text{ by case 2.}$$

□

Theorem 2. *Let $P = (r, s)$ be a point of prime order $p \geqslant 5$ on a generalized Hessian Curve $\mathsf{H}_{(\gamma,\delta)} : r^3 + s^3 + \gamma = \delta rs$ defined over $\mathbb{F}_{2^m}$, and n be a scalar multiple, with $2 \leqslant n \leqslant p-2$. Let $nP = (r_n, s_n)$ with $\mathfrak{r}_n = r_n^3 + s_n^3$ and $\mathfrak{r} = r^3 + s^3$. Then $\mathfrak{r}_n \neq \mathfrak{r}$.*

Proof. Let $\langle P\rangle$ be the group generated by P. As the order of P is a prime p, every non-identity element of $\langle P\rangle$ has order p. Let $\mathfrak{r} = \mathfrak{r}_n$.

1. P is a point of prime order $p \geqslant 5$, then $nP - P = (n-1)P$ can not be a point of order 3. Therefore, case 1 of Theorem 1 can not occur.
2. Without loss of generality, assume that $2 \leqslant n \leqslant p-2$. Then $3 \leqslant (n+1) \leqslant p-1$. Now let $nP - P = 2nP$. Then $(n+1)P = \mathcal{O}_H$, where $3 \leqslant (n+1) \leqslant p-1$, which contradicts that the order of the point P is p. Hence, case 2 of Theorem 1 can not happen.
3. Let $nP - P = 2nP + P_3$ where P_3 be a point of order three. Then we have $(n+1)P = P_3$. Therefore, $(n+1)P$ is also of order p. Therefore, p must be 3, which contradicts the hypothesis. □

3.1 Retrieve R and S coordinates

Let $P = (r, s)$ be a point on a generalized Hessian Curve $\mathsf{H}_{(\gamma,\delta)} : r^3 + s^3 + \gamma = \delta rs$ over a finite field $\mathbb{F}_{2^m}$ where $m \in \mathbb{N}$, and $n \geqslant 2$ be a scalar. Let $\mathrm{ord}(P) = p \geqslant 5$ and $\mathfrak{r} = r^3 + s^3 \neq 0$. Using Montgomery scalar multiplication, we compute $\mathfrak{r}_n = r_n^3 + s_n^3$ and $\mathfrak{r}_{n+1} = r_{n+1}^3 + s_{n+1}^3$ in the $\mathfrak{RT}$ coordinate where $\mathfrak{r}_n = r_n^3 + s_n^3$ and $\mathfrak{r}_{n+1} = r_{n+1}^3 + s_{n+1}^3$. Notice that $(n+1)P = nP + P$. Applying the addition formula (Equation (3) of [7]) of the generalized Hessian curve, we have $r_{n+1} = \frac{(s^2 r_n + s_n^2 r)}{(rs + r_n s_n)}$ and $s_{n+1} = \frac{(r^2 s_n + r_n^2 s)}{(rs + r_n s_n)}$. Therefore, we can write $\mathfrak{r}_{n+1}^3 = r_{n+1}^3 + s_{n+1}^3 = \frac{(s^2 r_n + s_n^2 r)^3}{(rs + r_n s_n)^3} + \frac{(r^2 s_n + r_n^2 s)^3}{(rs + r_n s_n)^3}$. After simplification, we apply $rs = \frac{\gamma + \mathfrak{r}}{\delta}$ and $r_n s_n = \frac{\gamma + \mathfrak{r}_n}{\delta}$, and we get

$$r_n^6 + \mathfrak{r} r_n^3 = \left(\mathfrak{r}_n^2 r^3 + r^6 \mathfrak{r}_n + \frac{1}{\delta^3}({\mathfrak{r}_n}^2 + \gamma^2)(\mathfrak{r} + \gamma)\mathfrak{r} + \frac{1}{\delta^3}(\mathfrak{r}_n + \gamma)(\mathfrak{r}^2 + \gamma^2)\mathfrak{r}_n + \frac{\mathfrak{r}_{n+1}(\mathfrak{r} + \mathfrak{r}_n)^3}{\delta^3} \right) / \mathfrak{r},$$

a quadratic equation in r_n^3. Let the roots be $r_{n,1}^3$ and $r_{n,2}^3$ with $r_{n,1}^3 + r_{n,2}^3 = \mathfrak{r}$.

1. **Let m be odd.** Then, using the relation $r_{n,i}^3 + s_{n,i}^3 = \mathfrak{r}_n$, we have two points $(r_{n,1}, s_{n,1}) = (r_{n,1}, (r_{n,1}^3 + \mathfrak{r}_n)^{1/3})$ and $(r_{n,2}, s_{n,2}) = ((r_{n,1}^3 + \mathfrak{r})^{1/3}, (r_{n,1}^3 + \mathfrak{r} + \mathfrak{r}_n)^{1/3})$. Let both the points $(r_{n,i}, s_{n,i})$ be on the curve $\mathsf{H}_{(\gamma,\delta)}$. Then, we have

$$\begin{aligned} & r_{n,1} s_{n,1} = r_{n,2} s_{n,2} = \frac{\gamma + \mathfrak{r}_n}{\delta}, \text{ from the equation of the curve } \mathsf{H}_{(\gamma,\delta)} \\ \Rightarrow\ & r_{n,1}^3 s_{n,1}^3 = r_{n,2}^3 s_{n,2}^3 \Rightarrow r_{n,1}^3 (r_{n,1}^3 + \mathfrak{r}_n) = (r_{n,1}^3 + \mathfrak{r})(r_{n,1}^3 + \mathfrak{r} + \mathfrak{r}_n) \Rightarrow \mathfrak{r}(\mathfrak{r} + \mathfrak{r}_n) = 0. \end{aligned}$$

   As $\mathfrak{r} \neq 0$, $\mathfrak{r} = \mathfrak{r}_n$. By Lemma 2, this contradicts the fact $\mathrm{ord}(P) \geqslant 5$, and it is a contradiction to the assumption that both the points $(r_{n,i}, s_{n,i})$ be on the curve $\mathsf{H}_{(\gamma,\delta)}$. Hence we can compute nP uniquely.
2. **Let m be even.** Using the relation $r_{n,i}^3 + s_{n,i}^3 = \mathfrak{r}_n$, we have six points $(r_{n,i,j}, s_{n,i,j})$ with $r_{n,i,j} = r_{n,i}\omega^j$ for all $i = 1, 2$ and $j = 0, 1, 2$ such that $r_{n,i,j}^3 + s_{n,i,j}^3 = \mathfrak{r}_n$. Let $(r_{n,1,j}, s_{n,1,j})$ and $(r_{n,2,j'}, s_{n,2,j'})$ be two points on $\mathsf{H}_{(\gamma,\delta)}$. Then, we get

$$\begin{aligned} & r_{n,1,j} s_{n,1,j} = r_{n,2,j'} s_{n,2,j'} = \frac{\gamma + \mathfrak{r}_n}{\delta}, \text{ from the equation of the curve } \mathsf{H}_{(\gamma,\delta)} \\ \Rightarrow\ & r_{n,1,j}^3 s_{n,1,j}^3 = r_{n,2,j'}^3 s_{n,2,j'}^3 \Rightarrow r_{n,1}^3 s_{n,1}^3 = r_{n,2}^3 s_{n,2}^3 \\ \Rightarrow\ & r_{n,1}^3 (r_{n,1}^3 + \mathfrak{r}_n) = (r_{n,1}^3 + \mathfrak{r})(r_{n,1}^3 + \mathfrak{r} + \mathfrak{r}_n) \Rightarrow \mathfrak{r}(\mathfrak{r} + \mathfrak{r}_n) = 0. \end{aligned}$$

   As $\mathfrak{r} \neq 0$, $\mathfrak{r} = \mathfrak{r}_n$. By Lemma 2, this contradicts the fact $\mathrm{ord}(P) \geqslant 5$. Therefore, either $(r_{n,1,j}, s_{n,1,j})$ or $(r_{n,2,j'}, s_{n,2,j'})$ is a point on the curve $\mathsf{H}_{(\gamma,\delta)}$, but not both. Without loss of generality, let us assume that for $(r_{n,1,1}, s_{n,1,1})$ be the point on the curve, and we get three points $(r_{n,1,j}, s_{n,1,j})$, $j = 0, 1, 2$ on the curve $\mathsf{H}_{(\gamma,\delta)}$. By Proposition 1 of [7], these three points are nP, $nP + P_3$ and $nP + 2P_3$, where P_3 is a point of order 3. Among these three points, nP has order p, and the other two have order $3p$. If p is known to us, we can uniquely determine the nP by computing the order of any two.

In order to avoid the computation of the order of a point, we can choose the scalar of the form $3n$. Now we can compute nP, and take any point from the above-mentioned three points. Then we compute $3nP$ with the fixed addition chain $(1, 1)$ at the cost of one standard addition and one standard doubling on a generalized Hessian curve. This way we can uniquely compute $3nP$ that is side-channel attack resistant.

For cryptographic purposes, we use $\mathbb{F}_{2^m}$ with m as prime [2, 9, 21, 15]. Except for 2, all the prime numbers are odd, and we can compute the nP uniquely from P, $\mathfrak{r}(nP)$, and $\mathfrak{r}((n+1)P)$ following the algorithm as given in Table 6.

Table 6. Compute nP from P, $\mathfrak{r}(nP)$ and $\mathfrak{r}((n+1)P)$ on $\mathsf{H}_{(\gamma,\delta)}$ over $\mathbf{F}_{2^m}$ with odd m

Input: The point $P = (r, s)$, $\mathfrak{r}(nP)$ and $\mathfrak{r}((n+1)P)$ Output: nP
1. Set $\mathfrak{r} = r^3 + s^3$.
2. If $\mathfrak{r} = 0$, Return $\perp$, else Continue;
3. Parse the input as $\mathfrak{r}_1 = \mathfrak{r}(P)$,$\mathfrak{r}_2 = \mathfrak{r}(nP)$, $\mathfrak{r}_3 = \mathfrak{r}((n+1)P)$
4. For $i = 1, 2$, Compute $\mathfrak{a}_i = \frac{\mathfrak{r}_i+\gamma}{\delta}$.
5. Compute $\mathfrak{c} = \left(\mathfrak{r}_2^2 r^3 + \mathfrak{r}_2 r^6 + \mathfrak{a}_1^2\mathfrak{a}_2\mathfrak{r}_2 + \mathfrak{a}_1\mathfrak{a}_2^2\mathfrak{r}_1 + \frac{\mathfrak{r}_3(\mathfrak{r}_1+\mathfrak{r}_2)^3}{\delta^3}\right)/\mathfrak{r}_1^3$
6. Compute $\mathfrak{h} = \mathfrak{r}_1 \times \text{HalfTrace}(\mathfrak{c})$.
7. If $\mathfrak{h}(\mathfrak{h} + \mathfrak{r}_2) = \left(\frac{\gamma+\mathfrak{r}_2}{\delta}\right)^3$ (As the cube roots here are unique)
8. Return $(r_n, s_n) = (\mathfrak{h}^{1/3}, (\mathfrak{h} + \mathfrak{r}_2)^{1/3})$
9. Else
10. Return $(r_n, s_n) = ((\mathfrak{h} + \mathfrak{r}_1)^{1/3}, (\mathfrak{h} + \mathfrak{r}_1 + \mathfrak{r}_2)^{1/3})$

4 Moving between Weierstrass curve and Generalized Hessian curve

A short Weierstrass curve $\mathsf{BEw}_{(a,b)}$ has an isomorphic Hessian curve if there exists a point of order three [26, 7]. We first move $\mathsf{BEw}_{(a,b)}$ to the triangular form of the Weierstrass curve, and then from the triangular form, the generalized Hessian has been derived. The existence of a triangular form relies on the existence of a point of order three on $\mathsf{BEw}_{(a,b)}$. In this work, our objective is to connect a binary Kummer line to a generalized Hessian curve, thus we will be using the short Weierstrass curve of the form $\mathsf{BEw}_{(b)}$. First, we discuss the existence of a point of order three on short Weierstrass curve $\mathsf{BEw}_{(b)}$. Then we discuss the isomorphic connection of the short Weierstrass curve to the generalized Hessian curve via Triangular form. As the second method, we show that we can connect $\mathsf{BEw}_{(b)}$ to a generalized Hessian curve using two isogenies. This guarantees an isogenous generalized Hessian curve just by choosing a binary Kummer line with a small coefficient c where the associated Weierstrass curve $\mathsf{BEw}_{(b)}$ has a

point of order three and the Hessian curve uses the same c in the arithmetic of Montgomery ladder step.

4.1 Moving between Weierstrass curve and Triangular Form

Let us start with the definition of the triangular form of the Weierstrass curve.

Definition 1. *[7] Let $a_3 \in \mathbb{F}_{2^m}$ and $a_3^3(a_3+1) \neq 0$. The projective form of the triangular Weierstrass curve over $\mathbb{F}_{2^m}$ is defined by*

$$\mathsf{BEwT}_{(a_3)} : \mathsf{Y}^2\mathsf{Z} + \mathsf{XYZ} + a_3\mathsf{YZ}^2 = \mathsf{X}^3. \tag{9}$$

Lemma 3. *Let $\mathsf{BEw}_{(b)}$ be defined over $\mathbb{F}_{2^m}$ and has a point of order 3 if and only if $x^4 + x^3 + b = 0$ has a root in $\mathbb{F}_{2^m}$, namely x_3, with $\mathrm{Tr}(x_3) = 0$.*

Proof. Let x_3 be a root of $x^4 + x^3 + b = 0$ with $\mathrm{Tr}(x_3) = 0$. There exists a point $P = (x_3, y_3)$ on $\mathsf{BEw}_{(b)}$ over $\mathbb{F}_{2^m}$ if y_3 is a root of the equation $y^2 + x_3y + (x_3^3 + b) = 0$. y_3 exists if and only if $\mathrm{Tr}\left((x_3^3 + b)/x_3^2\right) = 0$. Using $x_3^4 + x_3^3 + b = 0$ and the characteristic of the underlying field is two, we have $\mathrm{Tr}\left((x_3^3 + b)/x_3^2\right) = \mathrm{Tr}\left(x_3^4/x_3^2\right) = \mathrm{Tr}\left(x_3^2\right) = \mathrm{Tr}\left(x_3\right) = 0$. Therefore, $P = (x_3, y_3)$ is a point on $\mathsf{BEw}_{(b)}$ over $\mathbb{F}_{2^m}$. Now, we compute $2P = (x_2, y_2) = \left(x_3^2 + b/x_3^2, x_3^2 + (\eta + 1)x_2\right)$, where $\eta = x_3 + y_3/x_3$. Simplifying x_2 and y_2, we get $x_2 = x_3^2 + b/x_3^2 = (x_3^4 + b)/x_3^2 = x_3^3/x_3^2 = x_3$, and $y_2 = x_3^2 + (\eta + 1)x_2 = x_3^2 + (x_3 + y_3/x_3 + 1)\, x_3 = x_3 + y_3$. Therefore, we have $2P = (x_3, x_3 + y_3) = -P$, that is $3P = \mathcal{O}$.

Conversely, let $P = (x_3, y_3)$ be a point of order 3 on $\mathsf{BEw}_{(b)}$ over $\mathbb{F}_{2^m}$. Therefore, we have $3P = \mathcal{O}$, that is $2P = -P$. Equating the x-coordinates, we get $x_3^2 + b/x_3^2 = x_3$, that is, x_3 is a root of the equation $x^4 + x^3 + b = 0$. Also, y_3 is a root of the quadratic equation $y^2 + x_3y + (x_3^3 + b) = 0$, that implies $\mathrm{Tr}(x_3) = 0$. □

Remark 1. One can also find the cardinality of the elliptic curve $\mathsf{BEw}_{(a,b)}$, and if it is divisible by 3, then there is a point of order three by Cauchy's theorem. But this does not give the point explicitly, our approach does.

Lemma 4. *Let $\mathsf{BEw}_{(b)} : Y^2Z + XYZ = X^3 + bZ^3$ be a short Weierstrass elliptic curve defined over $\mathbb{F}_{2^m}$ with $b \neq 0$ containing a point of order 3, say $P = (x_3, y_3)$. Then $\mathsf{BEw}_{(b)}$ is isomorphic to the triangular Weierstrass elliptic curve $\mathsf{BEwT}_{(x_3)} : \mathsf{Y}^2\mathsf{Z} + \mathsf{XYZ} + x_3\mathsf{YZ}^2 = \mathsf{X}^3$ such that $x_3(1 + x_3) \neq 0$ and P maps to the point $(0 : 0 : 1)$.*

Proof. Consider the following map $\varrho : \mathsf{BEw}_{(b)} \to \mathsf{BEwT}_{(x_3)}$ [26]:

$$\varrho(X : Y : Z) \mapsto (\mathsf{X}, \mathsf{Y}, \mathsf{Z}) = (X + x_3Z : Y + \eta X + x_3^2 Z : Z), \text{ where } \eta = \frac{x_3^2 + y_3}{x_3} \tag{10}$$

The map ϱ is of the form $(u^2X + rZ : u^3Y + u^2sX + tZ : Z)$ with $u = 1, r = x_3, s = \eta$ and $t = x_3^2$. Therefore, this map forms an isomorphism [25, P. 44]. □

4.2 Moving between $\mathsf{BEwT}_{(a_3)}$ to $\mathsf{H}_{(\gamma,\delta)}$

[7, Theorem 1] provides similar maps given in Theorem 3. But the map of [7, Theorem 1] that corresponds χ_2 of Theorem 3 does not preserve the identity and thus is not an isomorphism. The next theorem follows the map given in [30] and provides the corrected version that fixes the identity and forms an isomorphism.

Theorem 3. *Let* $\mathsf{BEwT}_{(a_3)}: \mathsf{Y}^2\mathsf{Z}+\mathsf{XYZ}+a_3\mathsf{YZ}^2=\mathsf{X}^3$ *be a Weierstrass elliptic curve of triangular form with* $a_3 \in \mathbb{F}_{2^m}$ *and* $a_3^3(a_3+1)\neq 0$. *Then there exists a Generalized Hessian Curve* $\mathsf{H}_{(\gamma,\delta)}: R^3+S^3+\gamma T^3=\delta RST$ *that is isomorphic to* $\mathsf{BEwT}_{(a_3)}$.

Proof. We prove it in two parts based on whether m is odd or even.

1. **Let** m **be odd.** Every element of $\mathbb{F}_{2^m}$ has a unique cube root, and thus the $1+a_3$. Let ν be the cube root of $1+a_3$. As $\mathsf{char}=2\neq 3$, $\chi_1:\mathsf{BEwT}_{(a_3)}\rightarrow \mathsf{H}_{(\delta)}(=\mathsf{H}_{(1,\delta)})$ forms an isomorphism where $\delta=1/(1+\nu)$ by the Remark 1 of [7, Theorem 1]. χ_1 is as given below.

$$\left.\begin{aligned}\chi_1(\mathsf{X}:\mathsf{Y}:\mathsf{Z}) = (R:S:T)\\ R=\nu\mathsf{X}+\mathsf{Y}+a_3\mathsf{Z}\\ S=(1+\nu)\mathsf{X}+\mathsf{Y}\\ T=(1+\nu)\mathsf{X}+a_3\mathsf{Z}\end{aligned}\right\} \tag{11}$$

2. **Let** m **be even.** Now only one-third of the elements of $\mathbb{F}_{2^m}$ have a cube root, and $\mathsf{BEwT}_{(a_3)}$ is isomorphic to $\mathsf{H}_{(\delta)}$ by χ_1 whenever a_3+1 has a cube root. The map $\chi_2:\mathsf{BEwT}_{(a_3)}\rightarrow \mathsf{H}_{(1+a_3,1)}$ forms the isomorphism *when* a_3+1 *is not a cube.*

$$\left.\begin{aligned}\chi_2(\mathsf{X}:\mathsf{Y}:\mathsf{Z}) = (R:S:T)\\ R=\omega^2\mathsf{X}+\mathsf{Y}+a_3\omega\mathsf{Z}\\ S=\omega\mathsf{X}+\mathsf{Y}+a_3\omega^2\mathsf{Z}\\ T=\mathsf{X},\end{aligned}\right\} \tag{12}$$

where ω is a primitive cube root of 1. Even m ensures the existence of ω [6]. To resist GHS [10] and JV [15] attacks, finite fields with prime extensions are used for cryptographic purposes. We are interested in the map χ_1 because all primes except 2 are odd. □

4.3 Moving Between $\mathsf{BEw}_{(b)}$ and $\mathsf{H}_{(\gamma,\delta)}$ via Isomorphism

In this section, we now combine all the individual mappings short Weierstrass to and from triangular Weierstrass, and triangular Weierstrass to and from generalized Hessian. As a result, we achieve the necessary relations among short Weierstrass Curve $\mathsf{BEw}_{(b)}$ and generalized Hessian curve $\mathsf{H}_{(\gamma,\delta)}$.

Theorem 4. $\mathsf{BEw}_{(b)}: Y^2Z+XYZ=X^3+bZ^3$ *be a short Weierstrass curve such that* $x^4+x^3+b=0$ *has a root in* $\mathbb{F}_{2^m}$, *namely* x_3, *with* $\mathrm{Tr}(x_3)=0$. *Let* (x_3,y_3) *be a point of order 3 of* $\mathsf{BEw}_{(b)}$.

1. *If $1+x_3$ is a cube in $\mathbb{F}_{2^m}$ with the cube root ν, then $\mathsf{BEw}_{(b)}$ is isomorphic to a Hessian curve $\mathsf{H}_{(\delta=1/(1+\nu))} : R^3+S^3+T^3=\delta RST$ by the mapping*

$$\begin{aligned}\vartheta_1(X:Y:Z) = (R:S:T)\\ R &= (\nu x_3 + x_3^2 + y_3)X + x_3 Y + (\nu x_3^2 + \nu^3 x_3^2)Z\\ S &= (x_3 + y_3 + \nu x_3 + x_3^2)\mathsf{X} + x_3 Y + (\nu x_3^2 + \nu^3 x_3^2)Z\\ T &= x_3(1+\nu)X + \nu x_3^2 Z.\end{aligned}$$

2. *If $1+x_3$ does not have a cube root in $\mathbb{F}_{2^m}$, then $\mathsf{BEw}_{(b)}$ is isomorphic to a generalized Hessian curve $\mathsf{H}_{(\gamma=1+x_3,1)} : R^3+S^3+\gamma T^3 = RST$ by the mapping*

$$\begin{aligned}\vartheta_2(X:Y:Z) = (R:S:T)\\ R &= (\omega^2 x_3 + x_3^2 + y_3)X + x_3 Y + (x_3^3 + x_3^2)Z\\ S &= (\omega x_3 + x_3^2 + y_3)X + x_3 Y + (x_3^3 + x_3^2)Z\\ T &= x_3 X + x_3^2 Z,\end{aligned}$$

where ω is a primitive cube root of 1 in $\mathbb{F}_{2^m}$.

Proof. Let $\mathsf{BEw}_{(b)} : Y^2Z + XYZ = X^3 + bZ^3$ be a short Weierstrass curve. As $x_3 \in \mathbb{F}_{2^m}$ is a root of $x^4+x^3+b=0$ and $\mathrm{Tr}(x_3)=0$, $\mathsf{BEw}_{(b)}$ has a point of order 3 of the form $(x_3,\cdot)$ by Theorem(3). Let $P=(x_3,y_3)$ be a point order 3 that satisfies $\mathsf{BEw}_{(b)}$. Therefore, $\mathsf{BEw}_{(b)}$ is isomorphic to the triangular form of the Weierstrass elliptic curve $\mathsf{BEwT}_{(x_3)} : \mathsf{Y}^2\mathsf{Z} + \mathsf{XYZ} + x_3\mathsf{YZ}^2 = \mathsf{X}^3$ by mapping ϱ (Equation (10)) of Lemma 4.

1. If $1+x_3$ is a cube in $\mathbb{F}_{2^m}$, then $\mathsf{BEwT}_{(x_3)}$ is isomorphic to a Hessian curve $\mathsf{H}_{(\delta=1/(1+\nu))}$ by the mapping χ_1 from Theorem 3, where ν is a cube root of $1+x_3$. Composition of ϱ and χ_1 gives us $\vartheta_1 = \chi_1 \circ \varrho$, and makes the $\mathsf{BEw}_{(b)}$ isomorphic to a Hessian curve $\mathsf{H}_{(\delta=1/(1+\nu))}$.
2. $1+x_3 \in \mathbb{F}_{2^m}$ and $1+x_3$ is not a cube only if the extension degree m of $\mathbb{F}_{2^m}$ is even. Then $\mathsf{BEwT}_{(x_3)}$ is isomorphic to a generalized Hessian curve $\mathsf{H}_{(\gamma=1+x_3,1)}$ by the mapping χ_2 from Theorem 3. Similarly composing ϱ and χ_2, we get $\vartheta_2 = \chi_2 \circ \varrho$, and ϑ_2 makes $\mathsf{BEw}_{(b)}$ isomorphic to a generalized Hessian curve $\mathsf{H}_{(\gamma=1+x_3,1)}$. □

4.4 Moving between $\mathsf{BEw}_{(b)}$ and $\mathsf{H}_{(\gamma,\delta)}$ via Isogeny

To move between $\mathsf{BEw}_{(b)}$ and $\mathsf{H}_{(\gamma,\delta)}$, we define two isogenies with their duals: (i) ϕ is a 2-isogeny between $\mathsf{BEw}_{(b)}$ and $\mathsf{BEw}_{(\sqrt{b})}$, and (ii) ξ is a 3-isogeny between $\mathsf{H}_{(a^3,1)}$ and $\mathsf{H}_{(A,1)}$ with $A = a + a^2 + a^3$.

Theorem 5. *Let $\mathsf{BEw}_{(b)} : Y^2Z + XYZ = X^3 + bZ^3$ be a short Weierstrass curve defined on $\mathbb{F}_{2^m}$ where $b \in \mathbb{F}_{2^m}$ with $b \neq 0$. Then there exists an 2-isogeny $\phi : \mathsf{BEw}_{(b)} \mapsto \mathsf{BEw}_{(\sqrt{b})}$ defined by*

$$\phi(X:Y:Z) = (X^3 + \sqrt{b}XZ^2 : X^2Y + \sqrt{b}X^2Z + \sqrt{b}XZ^2 + \sqrt{b}YZ^2 + bZ^3 : X^2Z),$$

and the dual is

$$\hat{\phi}(\hat{X}:\hat{Y}:\hat{Z}) = (\hat{X}^2 : \hat{Y}^2 : \hat{Z}^2)$$

Proof. For simplicity, we use the affine form of $\mathsf{BEw}_{(b)} : y^2 + xy = x^3 + b$. As every element of $\mathbb{F}_{2^m}$ has a unique square root, $(0, \sqrt{b})$ is the point of order 2 on $\mathsf{BEw}_{(b)}$. Let G be the subgroup of order two generated by $(0, \sqrt{b})$. Using Velu's Formula [29] and Theorem 25.1.6 of [8], We construct an isogeny $\phi_1 : \mathsf{BEw}_{(b)} \to E'$, where $E' : y'^2 + x'y' = x'^3 + \sqrt{b}x' + \sqrt{b} + b$ as

$$\phi_1(x, y) = \left(\frac{x^3 + \sqrt{b}x}{x^2}, \frac{x^2 y + \sqrt{b}(x^2 + x + y)}{x^2} \right).$$

Secondly, we define the isomorphism $\phi_2 : E' \to \mathsf{BEw}_{(\sqrt{b})}$ as $(x', y') \mapsto (\hat{x} = x', \hat{y} = y' + \sqrt{b})$. The composition of ϕ_1 and ϕ_2 gives us the isogeny ϕ from $\mathsf{BEw}_{(b)}$ to $\mathsf{BEw}_{(\sqrt{b})}$ as

$$\phi(x, y) = (\phi_2 \circ \phi_1)(x, y) = \left(\frac{x^3 + \sqrt{b}x}{x^2}, \frac{x^2 y + \sqrt{b}(x^2 + x + y + \sqrt{b})}{x^2} \right). \quad (13)$$

The dual isogeny $\hat{\phi} : \mathsf{BEw}_{(\sqrt{b})} \to \mathsf{BEw}_{(b)}$ is defined by $\hat{\phi}(\hat{x}, \hat{y}) = (\hat{x}^2, \hat{y}^2)$, where

$$\begin{aligned}
(\hat{\phi} \circ \phi)(P = (x, y)) &= \left(x^2 + \frac{b}{x^2}, y^2 + b + \frac{b}{x^2} + \frac{by^2}{x^4} + \frac{b^2}{x^4} \right) \\
&= \left(x^2 + \frac{b}{x^2}, x^3 + xy + \frac{b}{x^2} + \frac{yb}{x^3} + \frac{b}{x} \right) \\
&= \left(x^2 + \frac{b}{x^2}, x^2 + \left(x + \frac{y}{x} \right) \left(x^2 + \frac{b}{x^2} \right) + \left(x^2 + \frac{b}{x^2} \right) \right) = 2P
\end{aligned}$$

Finally, the projective version of ϕ and $\hat{\phi}$ can be written as $\phi(X : Y : Z) = (X^3 + \sqrt{b}XZ^2 : X^2Y + \sqrt{b}X^2Z + \sqrt{b}XZ^2 + \sqrt{b}YZ^2 + bZ^3 : X^2Z)$ and the dual $\hat{\phi}(\hat{X} : \hat{Y} : \hat{Z}) = (\hat{X}^2 : \hat{Y}^2 : \hat{Z}^2)$. □

The form of the isogeny given by ξ in Theorem 6 appears in [30] without any proof, and also the dual is absent. Without the dual, we can not move in both directions. Theorem 6 completes the isogeny by giving the dual and the required proofs of isogeny and the dual.

Theorem 6. *Let* $\mathsf{H}_{(a^3,1)} : R^3 + S^3 + a^3T^3 = RST$ *be a generalized Hessian curve defined over* $\mathbb{F}_{2^m}$ *with* $a \neq 0$. *Then there exists a 3-isogeny* $\xi : \mathsf{H}_{(a^3,1)} \to \mathsf{H}_{(A,1)}$ *where* $A = a + a^2 + a^3$ *defined by*

$$\xi(R : S : T) = (a^2T^2S + aR^2T + S^2R : a^2T^2R + aS^2T + R^2S : RST),$$

and the dual is

$$\hat{\xi}(\hat{R} : \hat{S} : \hat{T}) = (a\hat{R}\hat{S}\hat{T} + \hat{S}^3 : (1 + a)\hat{R}\hat{S}\hat{T} + \hat{S}^3 + A\hat{T}^3 : \hat{R}\hat{S}\hat{T} + (1 + a + a^2)\hat{T}^3).$$

Proof. From the rational map $\xi : \mathsf{H}_{(a^3,1)} \to \mathsf{H}_{(A,1)}$, we have

$$\hat{R}^3+\hat{S}^3+A\hat{T}^3+\hat{R}\hat{S}\hat{T} = (aR^2S^2T^2+R^3S^3+a^3R^3T^3+a^3S^3T^3)(R^3+S^3+a^3T^3+RST).$$

Therefore, the range of ξ is indeed $\mathsf{H}_{(A,1)}$. Let $P = (R : S : T)$ and $\xi(P) = (1 : 1 : 0)$. Then we have $RST = 0$, and

1. If $R = 0$, then $a^2T^2S = aS^2T$, i.e. $aT = S$, and $P = (0, a, 1)$.
2. If $S = 0$, then $aR^2T = a^2RT^2$, i.e. $R = aT$, and $P = (a, 0, 1)$.
3. If $T = 0$, then $RS^2 = R^2S$, i.e. $R = S$, and $P = (1, 1, 0)$.

Therefore, the kernel of ξ is $\ker(\xi) = \{(1 : 1 : 0), (a : 0 : 1), (0 : a : 1)\}$, and makes ξ a 3-isogeny.

Now consider the rational map $\hat{\xi} : \mathsf{H}_{(A,1)} \to \mathsf{H}_{(a^3,1)}$ is defined by

$$\hat{\xi}(\hat{R} : \hat{S} : \hat{T}) = (a\hat{R}\hat{S}\hat{T} + \hat{S}^3 : (1+a)\hat{R}\hat{S}\hat{T} + \hat{S}^3 + A\hat{T}^3 : \hat{R}\hat{S}\hat{T} + (1+a+a^2)\hat{T}^3)$$

The $\hat{\xi}$ fixes the identity, and so $\hat{\xi}$ is an isogeny. Let $P = (R : S : T)$ be a point on $\mathsf{H}_{(a^3,1)}$. Let $(\hat{\xi} \circ \xi)(R : S : T) = (R_4 : S_4 : T_4)$ and $\Delta = R^3 + S^3 + a^3T^3 + RST$.

1. If $T \neq 0$, then we compute doubling and addition by Equations (6) and (5) of [7]. Let $3P = (R_3 : S_3 : T_3)$. Now

$$\begin{aligned} R_3 &= T(R_4) \\ S_3 &= T(S_4 + \Delta(a^3R^3T^3 + a^3S^3T^3 + R^3S^3)) \\ T_3 &= T(T_4 + \Delta((1+a)R^2S^2T^2 + a^3RST^4 + R^4ST + RS^4T)) \end{aligned}$$

   Therefore, $(\hat{\xi} \circ \xi)(R : S : T) = (R_4 : S_4 : T_4) = (R_3 : S_3 : T_3) = 3(R : S : T)$.
2. If $T = 0$, then addition by Equation (5) of [7] fails and produces $(0 : 0 : 0)$. In this case, we do addition by Equation (9) of [7]. Notice that, if $T = 0$ both R and S must be non-zero. Let $3P = (R'_3 : S'_3 : T'_3)$ and we have

$$\begin{aligned} R'_3 &= S(R_4) \\ S'_3 &= S(S_4 + \Delta(a^3R^3T^3 + a^3S^3T^3 + R^3S^3)) \\ T'_3 &= S(T_4 + \Delta((1+a)R^2S^2T^2 + a^3RST^4 + R^4ST + RS^4T)) \end{aligned}$$

   Therefore, $(\hat{\xi} \circ \xi)(R : S : T) = (R_4 : S_4 : T_4) = (R'_3 : S'_3 : T'_3) = 3(R : S : T)$.

This shows that $\hat{\xi}$ is the dual of ξ. □

Theorem 7. *Let* $\mathsf{BEw}_{(c^4)} : Y^2Z + XYZ = X^3 + c^4Z^3$ *be a short Weierstrass curve on* $\mathbb{F}_{2^m}$ *where* m *is odd and* $c(\neq 0) \in \mathbb{F}_{2^m}$*, and* $\mathsf{BEw}_{(c^4)}$ *has a point of order 3. Then there exists a generalized Hessian curve* $\mathsf{H}_{(\gamma,1)}$ *that is isogenous to* $\mathsf{BEw}_{(c^4)}$ *such that* $\sqrt{\gamma^3(\gamma+1)} = c$.

Proof. By Theorem 5, there exists an isogeny $\phi : \mathsf{BEw}_{(c^4)} \to \mathsf{BEw}_{(c^2)}$. $\mathsf{BEw}_{(c^4)}$ and $\mathsf{BEw}_{(c^2)}$ have the same cardinality by Theorem 1 of [28]. Therefore, $\mathsf{BEw}_{(c^2)}$ has a point of order 3, and let the point be (x_3, y_3). Then by Lemma 3, $x_3^4 + x_3^3 = c^2$. $\mathsf{BEw}_{(c^2)}$ is isomorphic to triangular form $\mathsf{BEwT}_{(x_3)}$ by the mapping ϱ of Lemma 4. The map χ_1 of Theorem 3 makes $\mathsf{BEwT}_{(x_3)}$ isomorphic to the generalized Hessian curve $\mathsf{H}_{(1,\delta)}$, where $\delta = \frac{1}{1+\nu}$ and $\nu^3 = 1 + x_3$, for odd m. Again, $\mathsf{H}_{(1,\delta)}$ is isomorphic to $\mathsf{H}_{\left(\frac{1}{\delta^3},1\right)} = \mathsf{H}_{((1+\nu)^3,1)}$ through the map φ (Equation (8)). By Theorem 6, there exists an isogeny $\xi : \mathsf{H}_{((1+\nu)^3,1)} \to \mathsf{H}_{(\gamma,1)}$, where $\gamma = (1+\nu) + (1+\nu)^2 + (1+\nu)^3 = 1 + \nu^3 = x_3$. Therefore, the composition $(\xi \circ \varphi \circ \chi_1 \circ \varrho \circ \phi)$ as given in Figure 1, we get that $\mathsf{H}_{(x_3,1)}$ is isogenous to $\mathsf{BEw}_{(c^4)}$ with $\sqrt{\gamma^3(\gamma+1)} = \sqrt{x_3^4 + x_3^3} = \sqrt{c^2} = c$. □

Figure 1 shows the diagrammatic view of the compositions of the maps and the connectivity of different curves.

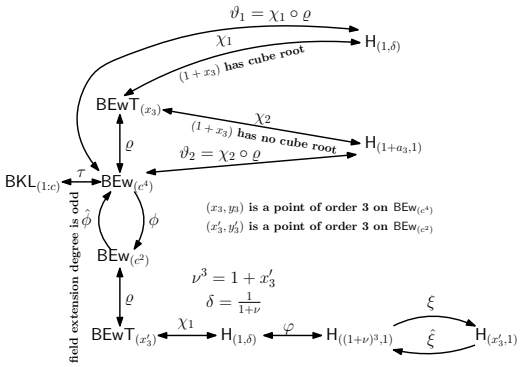

Fig. 1. All the paths of connection between Kummer and Hessian over binary field

4.5 Optimized Arithmetic on $\mathsf{H}_{(\gamma,1)}$

The $\mathsf{H}_{(\gamma,1)}$ obtained by Theorem 7 requires the smallest number of field operations. Let the $\mathfrak{RT}$-coordinates of P, Q, and $P-Q$ on $\mathsf{H}_{(\gamma,1)}$ be $(\mathfrak{R}_1, \mathfrak{T}_1), (\mathfrak{R}_2, \mathfrak{T}_2)$, and $(\mathfrak{R}, 1)$, respectively. $\mathfrak{RT}$-coordinate of $2P$ and $P+Q$ are $(\mathfrak{R}_3, \mathfrak{T}_3)$ and $(\mathfrak{R}_4, \mathfrak{T}_4)$ respectively. Applying $\delta = 1$ and $\sqrt{\gamma(\gamma^3+1)} = c$ in the arithmetic given in Table 3, we obtain new optimized arithmetic given in Table 7 that needs only $5[\mathsf{M}] + 4[\mathsf{S}] + 1[\mathsf{C}_s]$ operations in total.

5 Concrete proposal of curves

In the previous sections, we have established the relations among the Binary Kummer Lines and Hessian Curves. In this section, we apply all the results

Table 7. Mixed Doubling and Differential Addition on Binary $\mathsf{H}_{(\gamma,1)}$

$A = \mathfrak{R}_1 * \mathfrak{T}_2, B = \mathfrak{R}_2 * \mathfrak{T}_1, C = A * B, D = \mathfrak{R}_1^2, E = \mathfrak{T}_1^2, F = D + \sqrt{\gamma^3(1+\gamma)}E,$ $\mathfrak{R}_3 = F^2, \mathfrak{T}_3 = D * E, \mathfrak{T}_4 = (A+B)^2, \mathfrak{R}_4 = C + \mathfrak{R} * \mathfrak{T}_4$

derived till now to propose the appropriate pair of secure and practical curves which target 128-bit security over three binary fields: $\mathbb{F}_{2^{251}} = \mathbb{F}_2[t]/(t^{251} + t^7 + t^4 + t^2 + 1)$, $\mathbb{F}_{2^{257}} = \mathbb{F}_2[t]/(t^{257} + t^{12} + 1)$, and $\mathbb{F}_{2^{263}} = \mathbb{F}_2[t]/(t^{263} + t^9 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1)$. We choose these three particular fields as their extension degrees are all primes. Therefore the proposed curves are resistant to GHS attack [9] and JV attack [15].

Table 8. Pairs of Binary Kummer Lines and Binary Generalized Hessian Curves

Field	$\mathsf{BKL}_{(1:c)}$	$\mathsf{H}_{(1,\delta)}$	$(\log_2(p_1), \log_2(p_2))$	(h, h_T)	Bit Security
$\mathbb{F}_{2^{251}}$	$\mathsf{BKL}(\mathbf{251}, \mathbf{c_{1,1}})$	$\mathsf{H}(251, 1, \delta_1)$	(247.4,248.4)	$(12, 6)$	123.7
	$\mathsf{BKL}(251, c_{1,2})$	$\mathsf{H}(\mathbf{251}, \mathbf{1}, \delta_{\mathbf{2}})$			
$\mathbb{F}_{2^{257}}$	$\mathsf{BKL}(\mathbf{257}, \mathbf{c_{1,3}})$	$\mathsf{H}(257, 1, \delta_3)$	(253.4,254.4)		126.7
	$\mathsf{BKL}(257, c_{1,4})$	$\mathsf{H}(\mathbf{257}, \mathbf{1}, \delta_{\mathbf{4}})$			
$\mathbb{F}_{2^{263}}$	$\mathsf{BKL}(\mathbf{263}, \mathbf{c_{1,5}})$	$\mathsf{H}(263, 1, \delta_5)$	(259.4,260.4)		129.7
	$\mathsf{BKL}(263, c_{1,6})$	$\mathsf{H}(\mathbf{263}, \mathbf{1}, \delta_{\mathbf{6}})$			
$\mathbf{c_{1,1}}$=0x1bd9 $c_{1,2}$=0x760a53a3277bf1f5fe922cc529eb7e95922999fec51f300d6885642c40f067a $\mathbf{c_{1,3}}$=0x3c81 $c_{1,4}$=0x1073185a9d794b3ab04aade0f1fab315b290030dcce495e1a20afd1998b8557a $\mathbf{c_{1,5}}$=0x19001 $c_{1,6}$=0x1e491ff78af94d6ee907243a5dbd50922284849715d3ded4c70ff4e97a1d88e16f δ_1=0x4824661fb5bbc013eb1922d62f25db7e83f8553b40bbbfa29d2b333386e621 $\delta_{\mathbf{2}}$=0x326 δ_3=0x1cdb20e7787e32aa7b48e2287da944fcf4e313ec1bee64a440d047893b95fa2e4 $\delta_{\mathbf{4}}$=0x111d2 δ_5=0x4db5114bea200f30ccab250fa17cefc93c0eb4991bcf90c0b25d3683be619cf579 $\delta_{\mathbf{6}}$=0x9bbd					

We list six pairs of binary Kummer lines and binary generalized Hessian curves in Table 8. Here, $\mathsf{BKL}(m, c)$ denotes the $\mathsf{BKL}_{(1:c)}$ defined over $\mathbb{F}_{2^m}$ such that the corresponding $\mathsf{BEw}_{(c^4)}$ has a point of order 3, and $\mathsf{H}(m, \gamma, \delta)$ denotes the $\mathsf{H}_{(\gamma,\delta)}$ on the field $\mathbb{F}_{2^m}$ where $\gamma, \delta \neq 0$ and $\delta^3 \neq \gamma$. Observe that all the curves have a cofactor of $h = 12$, and the cofactor of the corresponding twist is $h_T = 6$. Let $\mathsf{BEw}_{(c_{1,1}^4)}$ be the associated short Weierstrass curve to $\mathsf{BKL}(251, c_{1,1})$. From [24] and the existence of a point of order 3, we have that

$\mathsf{BEw}_{(c^4_{1,1})}$ must have a cofactor divisible by 12. Let the cardinality of $\mathsf{BEw}_{(c^4_{1,1})}$ be $12p_2$, where p_2 is a prime. Then the cardinality of the twist of $\mathsf{BEw}_{(c^4_{1,1})}$ is $2^{m+1}+2-12p_2 = 2(2^m+1)-12p$, and is divisible by 2. Now the chosen m are odd, and thus $2^m \equiv 2 \pmod 3$, and (2^m+1) is divisible by 3. Therefore, the obtained cofactors are optimal. We first choose the smallest curve parameters (c or δ) for the boldfaced curve that achieves appropriate security. Next, we compute the rest of the values in that row. For example, consider the $\mathsf{BKL}(251, c_{1,1})$ and $\mathsf{H}(251, 1, \delta_1)$ pair. Here, we found that $c_{1,1}$=0x1bd9 is the smallest parameter for which we have optimal cofactor. Then the associated short Weierstrass curve is $\mathsf{BEw}_{(c^4_{1,1})}$, say (x_3, y_3). By Theorem 4, we have an isomorphic generalized Hessian curve $\mathsf{H}_{(1,\delta_1)}$ where $\delta_1 = 1/(1+\nu)$ and $\nu^3 = 1 + x_3$. On the other hand, consider the $\mathsf{BKL}(251, c_{1,2})$ and $\mathsf{H}(251, 1, \delta_2)$ pair. The inverse of the isomorphisms reveals that $\mathsf{H}_{(\gamma,\delta)}$ is isomorphic to $\mathsf{BEwT}_{\left(1/\delta_2+1/\delta_2^2+1/\delta_2^3\right)}$. Furthermore, it can be shown that $\mathsf{BEwT}_{\left(1/\delta_2+1/\delta_2^2+1/\delta_2^3\right)}$ has an isomorphic form $\mathsf{BEw}_{(b)}$ with $b = \left(1/\delta_2 + 1/\delta_2^2 + 1/\delta_2^3\right)^3 (1+1/\delta_2)^3$ if $\mathrm{Tr}(\frac{1}{\delta_2^3}) = 0$. Therefore, we choose the δ_2 as the smallest one such that $\mathrm{Tr}(\frac{1}{\delta_2^3}) = 0$ and we have optimal cofactor, and then $c^4_{1,2} = b$. This way of choosing a generalized Hessian curve is suggested by [7]. But for the curves $\mathsf{H}(\cdot, 1, \delta_i)$, $i = 2, 4, 6$, although δ_i^3 is small, $1/\sqrt{\delta_i^3}$ is not. Table 9 includes the binary Kummer line and generalized Hessian curve pairs where we choose the curves $\mathsf{H}(\cdot, \gamma_i, 1)$, $i = 1, 2, 3$, following the Theorem 6. The generalized Hessian curves of Table 9 provide the best operation counts mentioned in this article.

Table 9. Binary Generalized Hessian Curves

Field	$\mathsf{H}_{(\gamma,1)}$	$c = \sqrt{\gamma^3(\gamma+1)}$	$\mathsf{BKL}_{(1:c)}$	$(\log_2(p_1), \log_2(p_2))$	(h, h_T)	Bit Security
$\mathbb{F}_{2^{251}}$	$\mathsf{H}(\mathbf{251}, \gamma_\mathbf{1}, \mathbf{1})$	0x1bd9	$\mathsf{BKL}(251, c_{2,1})$	(247.4,248.4)	$(12, 6)$	123.7
$\mathbb{F}_{2^{257}}$	$\mathsf{H}(\mathbf{257}, \gamma_\mathbf{2}, \mathbf{1})$	0x3c81	$\mathsf{BKL}(257, c_{2,2})$	(253.4,254.4)		126.7
$\mathbb{F}_{2^{263}}$	$\mathsf{H}(\mathbf{263}, \gamma_\mathbf{3}, \mathbf{1})$	0x19001	$\mathsf{BKL}(263, c_{2,3})$	(259.4,260.4)		129.7
γ_1=0xee2ff990cc63e819c808dd80c72e8480cce06d2b345f5bed064dc11eac95f7 γ_2=0x1a60e52cdb75f34dd81a3d06572ad37d97244b45c383fd5af352f3d96bb681c40 γ_3=0x524570b33dddaa3eb326586232db22913ade54698e379dc9cb03258bfcf6be5571						

6 Conclusion

We provide a method to retrieve the R and S coordinates of the point nP obtained by the Montgomery ladder scalar multiplication in $\mathfrak{RT}$ coordinates of a generalized Hessian curve. We connect binary Kummer line to generalized Hessian curve via isomorphism and via isogeny. We also include new concrete proposals of binary Kummer lines and corresponding generalized Hessian curves that target 128-bit security levels and have small constants required for the arithmetic.

References

1. D. J. Bernstein. Curve25519: New Diffie-Hellman speed records. In *Public Key Cryptography - PKC*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006.
2. D. J. Bernstein. Batch binary edwards. In *Annual International Cryptology Conference*, pages 317–336. Springer, 2009.
3. D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange. Twisted hessian curves. In *International Conference on Cryptology and Information Security in Latin America*, pages 269–294. Springer, 2015.
4. I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.
5. W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions of Information Theory*, 22(6):644–654, 1976.
6. Faisala, Rojalia, and M. S. B. Mohamad. An Algorithm for Finding the Cube Roots in Finite Fields. In *5th International Conference on Computer Science and Computational Intelligence*, volume 109 of *Procedia Computer Science*, pages 838–844. Elsevier, 2021.
7. R. R. Farashahi and M. Joye. Efficient arithmetic on hessian curves. In *International Workshop on Public Key Cryptography*, pages 243–260. Springer, 2010.
8. S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.
9. S. D. Galbraith, F. Hess, and N. P. Smart. Extending the ghs weil descent attack. In *Advances in CryptologyâEUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28–May 2, 2002 Proceedings 21*, pages 29–44. Springer, 2002.
10. P. Gaudry, F. Hess, and Nigel Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15:19–46, 2002.
11. P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields and Their Applications*, 15(2):246–260, 2009.
12. D. Hankerson, A. J. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2010.
13. H. Hisil, K. Koon-Ho Wong, G. Carter, and E. Dawson. Twisted Edwards curves revisited. In *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *LNCS*, pages 326–343. Springer Berlin Heidelberg, 2008.
14. H. Huseyin and R. Joost. On Kummer Lines with Full Rational 2-Torsion and Their Usage in Cryptography. 45(4), 2019.
15. A. Joux and V. Vitse. Cover and Decomposition Index Calculus on Elliptic Curves Made Practical - Application to a Previously Unreachable Curve over $\mathbb{F}_{p^6}$. In *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 9–26. Springer, 2012.
16. M. Joye and J. Quisquater. Hessian elliptic curves and side-channel attacks. In *International workshop on cryptographic hardware and embedded systems*, pages 402–410. Springer, 2001.
17. S. Karati. Binary kummer line. In *Applied Cryptography and Network Security - 21st International Conference, ACNS 2023, Kyoto, Japan, June 19-22, 2023, Proceedings, Part I*, volume 13905 of *LNCS*, pages 363–393. Springer, 2023.

18. S. Karati and P. Sarkar. Connecting legendre with kummer and edwards. *Adv. Math. Commun.*, 13(1):41–66, 2019.
19. S. Karati and P. Sarkar. Kummer for Genus One Over Prime-Order Fields. *Journal of Cryptology*, pages 1–38, 2019. `https://doi.org/10.1007/s00145-019-09320-4`.
20. N. Koblitz. Elliptic Curve Cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.
21. A. Menezes and M. Qu. Analysis of the weil descent attack of gaudry, hess and smart. In *Cryptographersâ Track at the RSA Conference*, pages 308–318. Springer, 2001.
22. V. S. Miller. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology - CRYPTO*, LNCS, pages 417–426. Springer, 1985.
23. K. Nath and P. Sarkar. Kummer versus montgomery face-off over prime order fields. *ACM Trans. Math. Softw.*, 48(2):13:1–13:28, 2022.
24. T. Pornin. Efficient and complete formulas for binary curves. Cryptology ePrint Archive, Paper 2022/1325, 2022. `https://eprint.iacr.org/2022/1325`.
25. J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.
26. N. P. Smart. The hessian form of an elliptic curve. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 118–125. Springer, 2001.
27. M. Stam. On montgomery-like representations for elliptic curves over gf (2 k). In *Public Key CryptographyâPKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings 6*, pages 240–254. Springer, 2002.
28. J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.
29. J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, juillet 1971.
30. M. Wroński and T. Kijko. Arithmetic on generalized hessian curves using compression function and its applications to the isogeny-based cryptography. *Publ. Math. Debrecen*, page 655â682, 2022. DOI: 10.5486/PMD.2022.Suppl.7.