Received: July 24, 2023. Revised: September 3, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Enhanced Performance of Isogenies Over Huff Curve for Post Quantum Cryptography

Akash Rathor[1] Manoj Kumar[1]* R. K. Mishra[2] Shivender Goswami[1] Ankit Chaudhary[1]

[1]*Department of Mathematics and Statistics, Gurukula Kangri (Deemed to be University), 249404, Haridwar (Uttarakhand), India*
[2]*Department of Applied Science and Humanities, GL Bajaj Institute of Technology and Management, 201306, Greater Noida, India*
* Corresponding author's Email: sdmkg1@gmail.com

Abstract: Artificial intelligence and machine learning, as intelligent systems, have a vital role to play in both the development and deployment of solutions for post-quantum cryptography. Post-quantum cryptography's (PQC's) most important aspect is cryptography based on isogeny (IBC). It is extensively used because of its compatibility and shorter key lengths. Point operations and isogeny computations are used as the basic building blocks in the implementation of the IBC. SIDH (supersingular isogeny diffie-hellman) and CSIDH (commutative supersingular isogeny diffie-hellman) finds application in isogeny-based cryptography for the provision of secure key exchange protocols and cryptographic primitives. The isogeny degree holds great significance in both SIDH and CSIDH schemes, serving as a critical parameter that profoundly impacts the security and efficiency of these cryptographic protocols built upon isogenies. In actual IBC implementations, where decreasing computational overhead can greatly enhance system performance. Montgomery curves are used in the literature because they can be used to carry out a specialised point operation. Methods for calculating 2, 3, and 4 isogenies on the Huff curve have been proposed in the current study. These techniques include changing an affine plane into a projective plane. In terms of computational cost, the study discovered that the suggested methods for computing isogenies on the Huff curve are more effective than those utilising the Edwards and Montgomery curves.

Keywords: Velu's formulae, Isogeny-based cryptography, Elliptic curves, Post-quantum cryptography.

1. Introduction

In the realm of post-quantum cryptography, intelligent systems have a pivotal role to play. They elevate the refinement, analysis, execution, and supervision of secure cryptographic algorithms and protocols, which are essential safeguards against the growing potential of quantum computing. Intelligent systems have a substantial impact on various dimensions of post-quantum cryptography, such as algorithm creativity, secure key management, threat recognition, and enabling quantum-safe infrastructures. Problems based on the discrete logarithm or integer factorization would no longer be viewed as intractably difficult if Shor's method were used sufficiently broadly in a quantum computer. The popularity of PQC is rising as a result of the advent of quantum computers. It is beneficial for binary-digit-based cryptosystems and will continue to be secure against a quantum attacker. Because IBC employ very small keys and require less power, they are considered to be more effective than those that were previously in use. When De Feo and Jao [1] initially established the SIDH protocol, IBC began to gain popularity. The security of the SIDH protocol is based on how challenging it is to detect the isogeny. In actuality, the concept of isogeny under an ordinary curve was first presented by Couveignes [2], which Stolbunov [3] further reanalyzed. The algorithm was ineffective in practice in addition to being vulnerable to the sub-exponential attack by the quantum

Table. List of symbols used in this paper

Symbol	Description	Symbol	Description
F_p	Field with characteristics p	ℓ_A, ℓ_B	Prime numbers
e_A, e_B	Natural numbers	ℓ_i	Prime numbers greater than 2
$\tilde{O}(\ell)$	Order in quaternion algebra	w	Symbol for projective plane
ℓ	odd prime	m_A, m_B	Two coprime natural numbers
q	Prime number	f	Integer co-factor
m, e	$m \in \{m_A, m_B\}, e \in \{e_A, e_B\}$	P_A, Q_A, P_B, Q_B	Points on elliptic curve
ℓ_A, n_A	Random elements in $\mathbb{Z}/{m_A}^{e_A}\mathbb{Z}$	R_A	A set span by the points P_A, Q_A
Φ_A	An isogeny from E to E_A	E_A	A curve $E/< R_A >$
$\Phi_A(P_B), \Phi_A(Q_B), \Phi_B(P_A), \Phi_B(Q_A)$	Points on image curve	$R`_A$	A set span by the points $\Phi_B(P_A), \Phi_B(Q_A)$
E_{AB}, E_{BA}	Elliptic curves	Θ	imaginary-quadric order
$\mathcal{E}\ell\ell_q(\Theta)$	set of elliptic curves formed over field F	$Cl(\Theta)$	Class group action
[c]	An ideal class in $Cl(\Theta)$	m_i	Odd primes
$End_q(E)$	Endomorphism ring of an elliptic curve	$H_{a,b}$	Huff curve with curve coefficient a, b
$G_{a,b}$	General Huff curve with curve coefficient a, b	H_c	Huff curve with curve coefficient c
r, s	Coordinates of curve	$\dot{O}$	Identity point
$W_{A,B}$	Short Weierstrass curve with curve coefficient A, B	E_d	Edwards curve with curve coefficient d
M_D	Montgomery curve with curve coefficient D	r_m, r_l, r_n s_m, s_l, s_n	Coordinates of point $L, M, L+M$
$W_{\gamma,\delta}$	Short Weierstrass curve with curve coefficient $\gamma,\ \delta$	$M_{C,D}$	Montgomery curve with curve coefficient C, D
E_1, E_2	Two elliptic curves	m	Isogeny degree
Φ	Isogeny between E_1, E_2	$\hat{\Phi}$	Dual isogeny of Φ
K	Field	E'	Where $E' = E/G$
G	Finite set of points on E	$Ker\ \Phi$	Kernel of an isogeny Φ
$r_P,\ s_P, r_Q, s_Q, r_{P+Q}, s_{P+Q}$	Co-ordinates points of $P, Q, P+Q$	G^+, G^-	Two partitions of G
R, S, T, R', S', T'	Projective coordinates	$R_M, S_M, T_M, R_0, S_0, T_0$	Projective coordinates of points $P, 2P$
ι	An isomorphism from $M_{A,B}$ to E	ψ	An isogeny from image curve to $M_{A',B'}$
Φ_1	Isogeny between $M_{A',B'}$ to $M_{A'',B''}$	ψ'	Isogeny between $M_{A'',B''}$ to $H_{a,b}$
α_i, β_i	Coordinates point on Huff curve	a', b'	Image curve coefficients of Huff curve
s_2, m_2, a_2	Field squaring, multiplication, and addition operations		

computer [4]. However, Childs et al. [5] presented a quantum sub-exponential assault, making their method susceptible, and the suggested solution makes use of the commutative property of endomorphism rings. The approach proposed in [5] could not work. SIKE (Super-singular Isogeny Key

Encapsulation) was a different method for the NIST standardisation effort in 2017 [5]. When compared to PQC primitives, which are distinct from isogeny-based cryptosystems but still maintain the same level of security, an isogeny-based cryptosystem's key size is smaller. Its implementation, however, moves more slowly than that of any other option for the NIST programme. The key exchange process for SIDH was first introduced in 2016 by Azarderakhsh et al. [6, 7]. The most advanced computing method for SIKE is still that introduced by Costello et al. [8]. Seo et al. [9] developed a rapid modular arithmetic multiplication approach for the SIDH protocol and the SIKE protocol in 2018. The only curve on which faster point arithmetic and efficient isogeny enumeration can be performed is Montgomery curve.

Until now we couldn't find the elliptic curve model which is faster than the Montgomery curve. The CRS (couveignes, rostotsev, and stolbunov) scheme has been studied independently by De Feo et al. [10] and also Castryck et al. [11]. Castryck et al. [11] CRS scheme more modified. Super-singular elliptic curves built over F_p were used in [11] to resolve the parameter selection problems in the CRS system. CSIDH is currently slower than SIDH, taking 80ms on the 128-bit classically computer security level, but one of its primary advantages is that it may be used to build a reasonably strong digital signature [12]. CSI-FiSh [12] offered a workable digital signature that takes 390 ms to apply to a message. An isogeny degree in IBC is calculated using a prime. In the SIDH protocol, the form of the prime number p is here, and these are the prime numbers with a cofactor of 1. The values of and represent the degrees of the isogenies used in the protocol. Typically, implementations of IBC use isogenies of degrees three and four. In the CSIDH algorithm, the form of the prime number p is, where are primes greater than or equal to 3. The numerical value of relates to the magnitude of an isogeny that is utilised within the algorithm. The CSIDH scheme relies on isogenies of varying degrees, thus necessitating an efficient formula for odd-degree isogeny, particularly since the advent of the CSIDH algorithm. In the field of elliptic curve cryptography, finding an arbitrary odd-prime degree isogeny on a Montgomery curve is a challenging task. However, Costello and Hisil [13] have developed an efficient method to overcome this challenge. In traditional methods, calculating ℓ-isogeny requires $\tilde{O}(\ell)$. But, by the using the square-root Vélu formula introduced by Bernstein et al. [14], the computation complexity can be reduced to $\tilde{O}(\sqrt{\ell})$. An efficient method for finding isogenies of substantial odd-degree that is applicable to B-SIDH and CSIDH has also been proposed in a recent work [15]. Recent studies in quantum computing have shown that using isogenies of large numbers of odd-degrees is critical to ensuring big-level security [16, 17]. Therefore, the method proposed in [15] can significantly enhance the security of IBC. This is why most IBC implementations are based on Montgomery curves. Moreover, the current leading implementation in this domain, proposed in reference [18], also employs Montgomery curves as its basis. Twisted Edwards curves are one type of elliptic curve that are birationally equivalent to Montgomery curves and can be transformed from one curve to the other using projective coordinates. The pioneering work of Meyer et al. [19] involved using Edwards curves for isogeny computation while performing elliptic curve arithmetic using Montgomery curves. Using Montgomery and Edwards curves for elliptic curve arithmetic and isogeny calculation, respectively, the method was further refined in reference [18]. However, earlier studies [18, 19] and [20, 21] have shown that solely employing Edwards curves to develop SIDH-based techniques performs worse than those that merely use Montgomery curves. Conversely, the superiority of Edwards curves becomes more evident when deploying CSIDH-based algorithms, which involve utilising a greater number of odd-degree isogenies compared to SIDH-based algorithms.

Although finding the image curve's coefficient on Montgomery curves might be challenging, it's much simpler on Edwards curves used by Meyer et al. in [22]. Furthermore, Kim et al. improved the isogeny technique for odd-degree isogenies by employing the Edwards curve's w-coordinate in reference [23]. By modifying the formula in [23], one can achieve faster Edwards-only CSIDH as compared to Montgomery-CSIDH or hybrid-CSIDH. Some isogeny-based algorithms may perform better on a particular elliptic curve, according to reference [23].

Recently, Broon et al. proposed an optimized formula for isogenies between Hessian model (twisted) of elliptic curves in [24]. In the Montgomery type of elliptic curve, B-SIDH speed is determined by using a new technique to enumerate l-isogeny curve developed by Huang et al. [25]. Zhi hu et al. [26] proposed w-coordinate model, 2-isogeny and odd degree isogenies on Jacobi quartic (extended) curve. Dey et al. [27] constructed the first syncryption using IBC. Zheng Tao et al. [28] proposed a w-coordinate system on Twisted Hessian curve.

In the work of Meyer et al. [18], the 2-isogeny formula was first introduced for the Montgomery curve, with an associated computational expense

noted as $2s_2 + 4m_2 + 5a_2$ building on this, Costello and Smith presented a more generalized 3-isogeny formula for the Montgomery curve in their research [19], with a corresponding computational cost referred to as $5s_2 + 6m_2 + 14a_2$. Azarderakhsh et al. contributed to this area by outlining a distinct 2-isogeny formula for the Edwards curve, tied to a computational cost denoted as $3s_2 + 31m_2$ in their publication [29]. In a similar vein, Kim et al. put forth a generalized 3-isogeny formula for the Edwards curve, with a designated computational cost $6m_2 + 5s_2 + 11a_2$ in their study [30]. In the context of our current study, we have conducted optimizations on the general formulas for 2, 3, and 4-isogenies, focusing specifically on Huff curves. Additionally, our analysis encompasses a comprehensive comparison of formula expenses across the Montgomery, Edwards, and Huff curve variations. In terms of computational efficiency, the study's findings demonstrate that the proposed methods for computing isogenies on the Huff curve exhibit superior effectiveness compared to those utilised for the Edwards and Montgomery curves.

In this research, we utilize various methods including birational transformation, homomorphism properties, and affine-to-projective transformation to enable the computation of two, three, and four isogenies, as well as the evaluation of coefficients. Our findings, supported by a comparative bar chart, demonstrate that the operational cost of the huff curve is comparable to that of the Montgomery curve, while offering improved operational cost compared to the Edwards curve.

This paper is structured as follows. Section 2 offers a comprehensive review of the huff curves, SIDH-CSIDH scheme, and Velu's formula to provide background context. In section 3, we introduce the w-coordinate system and present enhancements to the two, three, and four isogeny. The algorithm and cost of computing the isogeny computation and coefficient evaluation are described in section 4. We also include a bar chart comparison in this section. Finally, section 5 concludes the paper and outlines future prospects.

2. Preliminaries

The purpose of this part is to give an overview of certain key ideas that are necessary to understand the suggested scheme. Firstly, we introduce the two primary streams of IBC, namely SIDH and CSIDH. SIDH is a PQC scheme that relies on the isogeny problem.

2.1 IBC

This paragraph briefly introduces the topic of key-exchange protocols for SIDH and CSIDH and mentions two cited sources, [10, 11], which provide a detailed study of these protocols.

2.1.1. SIDH scheme

To establish a key exchange protocol, it is necessary to choose two fixed coprime numbers, denoted as m_A and m_B. Let e_A and e_B be positive integers such that ${m_A}^{e_A}$ is approximately equal to ${m_B}^{e_B}$. It is decided to choose a prime number q here $q = {m_A}^{e_A}{m_B}^{e_B} f \pm 1$, here f is an integer co-factor. An order $({m_A}^{e_A}{m_B}^{e_B} f)^2$ over the finite field $\mathbb{F}_{q^2}$ is then created. For each $m \in \{m_A, m_B\}$ and each $e \in \{e_A, e_B\}$, we obtain a complete set of all point of m^e-torsion on E upon $\mathbb{F}_{q^2}$. Two bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$, are chosen for the set of all point of ${m_A}^{e_A}$ and ${m_B}^{e_B}$-torsion, respectively.

Assuming that Alic and Bibi want to interchange private keys and their chosen bases are $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$, respectively. Alic selects random elements $l_A, n_A \in \mathbb{Z}/{m_A}^{e_A}\mathbb{Z}$ that cannot both be divided by m_A, computes the set $< R_A >= < [l_A]P_A + [n_A]Q_A >$ for key generation. Using Vélu's formula (VLF), Alic calculates a curve $E_A = E/< R_A >$ and an isogeny $\Phi_A: E \to E_A$ of degree ${m_A}^{e_A}$, where $ker\Phi_A =< R_A >$. Alic and Bibi perform the same calculation to establish a shared secret key. Alic sends Bibi the values $\left(E_A, \Phi_A(P_B), \Phi_A(Q_B)\right)$, and Bibi sends Alic the values $(E_B, \Phi_B(P_A), \Phi_B(Q_A))$. To establish the key, Alic calculates the subgroup $< R`_A >= < [l_A]\Phi_B(P_A) + [n_A]\Phi_B(Q_A) >$ and then calculates a curve $E_{AB} = E_B/< R`_A >$ using VLF. Similarly, Bibi calculates the curve $E_{BA} = E_A/< R`_B >$ using the same method as Alic. The j-invariants of the curve E_{BA}, E_{AB} are equivalent that provides the shared-secret key between Bibi and Alic.

2.1.2. CSIDH scheme

In the CSIDH protocol, super-singular elliptic type curves (SEC) are subjected to a commutative-group action over a finite field $\mathbb{F}_q$. The imaginary-quadric order is denoted by Θ, and $\mathcal{E}\ell\ell_q(\Theta)$ is the set of elliptic curves formed over $\mathbb{F}_q$ with an endomorphism ring. An open and transitive class group on $\mathcal{E}\ell\ell_q(\Theta)$ is notified by $Cl(\Theta)$. The group action or CM-action of an ideal class $[\mathfrak{c}] \in Cl(\Theta)$ on an elliptic curve $E \in \mathcal{E}\ell\ell_p(\Theta)$ is denoted by $[\mathfrak{c}]E$. To generate a prime, small separate odd primes $m_1, m_2, m_3, \ldots, m_n$ are used, such that $q =$

$4m_1m_2m_3m_4 \ldots\ldots m_n - 1$. The endomorphism ring $End_q(E)$ of an SEC E is equal to $\mathbb{Z}[\pi]$. It should be noted that the quaternion order $End(E)$ subring in $End_q(E)$ is commutative. When the Frobenius trace is zero, it results in $E(\mathbb{F}_q) = q + 1$. The ideal $m_i(\Theta)$ splits into $\mathfrak{l}_i\bar{\mathfrak{l}}_i$ because of $\pi^2 - 1 = 0\ mod\ m_i$, where $\mathfrak{l}_i = (m_i, \pi - 1)$ and $\bar{\mathfrak{l}}_i = (m_i, \pi + 1)$. By using the Velu's Formula, the group action $[\mathfrak{l}_i]E\ (resp.\ [\bar{\mathfrak{l}}_i]E)$ can be calculated through isogeny $\Phi_{\mathfrak{l}_i}$ over $\mathbb{F}_q$ (resp. $\Phi_{\bar{\mathfrak{l}}_i}$). Take the scenario where Bibi and Alic wish to transfer a secret key. Alic selects an element (vector) $(e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$, where $e_i \in [-l, l]$ for a natural number l. This vector denotes an isogeny connected by the group action of the ideal class $[\mathfrak{c}] = [{\mathfrak{l}_1}^{e_1} \ldots {\mathfrak{l}_n}^{e_n}]$, where $\mathfrak{l}_i = (m_i, \pi - 1)$. After Alic calculates the public key $E_A := [\mathfrak{c}]E$, Bibi receives E_A. Using his own private ideal b, Bibi executes a similar process and transmits Alic the resultant public key, $E_B := [\mathfrak{b}]E$. As soon as Bibi's public key is received, Alic calculates $[\mathfrak{c}]E_B$, while Bibi calculates $[\mathfrak{b}]E_A$. Since $[\mathfrak{c}]E_B$ and $[\mathfrak{b}]E_A$ are isomorphic by reason of commutativity, the elliptic curves can be used to access the shared secret data.

The Huff curves' arithmetic

In IBC, Montgomery curves have been widely used due to their computational efficiency. One such type is the Huff curve, which has shown promising results in terms of arithmetic computations and can be a strong contender compared to Montgomery curves.

2.1.3. Huff curves

Joye et al. introduced and elucidated the concept of Huff models for elliptic curves in their paper [31]. Tate pairings were calculated using a group law and a formula published in that publication. The Huff representation of an elliptic curve is described by:

$$H_{a,b}; ar(s^2 - 1) = bs(r^2 - 1) \tag{1}$$

With properties $a^2 \neq b^2$, a and b are non-zero, and the point $\dot{O} = (0,0)$ is the identity element, $-(r, s) = (-r, -s)$. Also, K is a finite field with a characteristic greater than 2. It is noteworthy that each Huff curve have three points of order two located at infinity. One viable method of simplifying the Huff curve $H_{a,b}$ is by using the following approach:

$$H_c; cr(s^2 - 1) = s(r^2 - 1) \tag{2}$$

Where $c = \frac{a}{b}, c \neq \pm 1$. Reference [32] introduces the concept of generalized Huff curves, which encompasses the Huff form of elliptic curves and can be defined by the following equation:

$$G_{a,b}; r(as^2 - 1) = s(br^2 - 1) \tag{3}$$

where $a \neq b$ and $a, b \neq 0$. The point $\dot{O} = (0,0)$ is the identity element, $-(r, s) = (-r, -s)$. The $j-$invariant of the curve $G_{a,b}$ is

$$jG_{a,b} = \frac{2^8(a^2 - ab + b^2)^3}{a^4b^4(a - b)^2},$$

and the curve $H_{a,b}$`s $j-$invariant is

$$jH_{a,b} = \frac{2^8(a^4 - a^2b^2 + b^4)^3}{a^4b^4(a^2 - b^2)^2}.$$

2.1.4. Isomorphism

The curve $H_{a,b}$ can be transformed into different types of elliptic curves that are well-studied in cryptography. For instance, $H_{a,b}$ is isomorphic to a Weierstrass curve of the form

$$W_{A,B}: s^2 = r^3 + Ar^2 + Br \tag{4}$$

where $A = (a^2 + b^2)$ and $B = a^2b^2$. It is also isomorphic to an Edwards curve of the form

$$E_d: r^2 + s^2 = 1 + dr^2s^2 \tag{5}$$

where $d = ((a - b)/(a + b))^2$. Finally, $H_{a,b}$ is isomorphic to a Montgomery curve of the form

$$M_D;\ s^2 = r^3 + Dr^2 + r \tag{6}$$

where $D = (a^2 + b^2)/ab$.

2.1.5. Arithmetic on Huff curves

The addition of two points $L + M = (r_n, s_n)\ (where\ L = (r_m, s_m)\ and\ M = (r_l, s_l))$ on the Huff curve $H_{a,b}$ can be computed using a specific formula, as given below. Moreover, the same formula can be used to double a point on the curve.

Adding of two points on $H_{a,b}$ is determine by the following formula

$$r_n = \frac{(r_m + r_l)(1 + s_m s_l)}{(1 + r_m r_l)(1 - s_m s_l)} \tag{7}$$

$$s_n = \frac{(s_m + s_l)(1 + r_m r_l)}{(1 + s_m s_l)(1 - r_m r_l)} \tag{8}$$

The formula used for addition in the Huff curve H_c is same. The general Huff curve $G_{a,b}$ follows a similar process to compute the unified sum.

$$r_n = \frac{(r_m+r_l)(as_ms_l+1)}{(br_mr_l+1)(as_ms_l-1)} \quad (9)$$

$$s_n = \frac{(s_m+s_l)(br_mr_l+1)}{(as_ms_l+1)(br_mr_l-1)} \quad (10)$$

Where $L = (r_m, s_m)\ and\ M = (r_l, s_l)$ are the points on $G_{a,b}$ and $L + M = (r_n, s_n)$.

Theorem [33]. Every elliptic curve with three *points of order Two* is isomorphic to a general Huff curve.

2.2 Designs for the elliptic curve

The riemann-roch theorem states that an elliptic curve can be represented by a polynomial equation in a pair of variables having a degree equal to three and a field with characteristic K greater than 3. One such representation of an elliptic curve is through a short Weierstrass equation.

$$W_{\gamma,\delta}:\ s^2 = r^3 + \gamma r + \delta \quad (11)$$
$$4\gamma^3 + 27\delta^2 \neq 0$$

or by a Montgomery curve equation

$$M_{C,D}:\ Ds^2 = r^3 + Cr^2 + r \quad (12)$$
$$D(C^2 - 4) \neq 0$$

The j-invariants are notified as $j(W_{\gamma,\delta}) = 1728 \cdot \frac{4\gamma^3}{(4\gamma^3+27\delta^2)}$ and $j(M_{C,D}) = 256\frac{(C^2-3)^3}{(C^2-4)}$. Weierstrass equation or the Montgomery equation can be used to depict an elliptic curve; the former is known as the weierstrass model. Both models are required to use elliptic curves for cryptographic purposes. The points of order four or three points of order two can be found in $M_{C,D}$ (possibly both), as mentioned in [34, 35].

A curve represented in the $H_{a,b}$ form can be transformed into the Weierstrass form through a direct and uncomplicated birational transformation, as stated in [36]. This transformation is described by the map

$$(r, s) = \left(\frac{br-as}{s-r}, \frac{b-a}{s-r}\right) \quad (13)$$

And the resulting curve equation is $s^2 = r^3 + (a + b)r^2 + abr$ in the weierstrass form. Conversely, to obtain the $H_{a,b}$ form from the weierstrass form, the inverse transformation formula is

$$(r, s) = \left(\frac{r+a}{s}, \frac{r+b}{s}\right) \quad (15)$$

Similarly, a curve represented in the $M_{C,D}$ form can be transformed into the weierstrass form using a straightforward birational transformation, as mentioned in [34]. The transformation is given by the map

$$(r, s) = \left(\frac{r}{D}, \frac{s}{D}\right) \quad (16)$$

And the resulting curve equation is $s^2 = r^3 + \frac{C}{D}r^2 + \frac{1}{D^2}r$ in the Weierstrass form. To obtain the $M_{C,D}$ form from the Weierstrass form, the inverse transformation formula is also available.

$$(r, s) = \left(\frac{r}{\sqrt{b}}, \frac{s}{\sqrt{b}}\right) \quad (17)$$

2.3 Calculations by isogeny and Velu's formulae

An isogeny defines a group morphism with a finite number of kernel members that translates E_1 onto E_2. If there exists an isogeny between two elliptic curves E_1 and E_2, both are isogenous. If the degree of the isogeny equals the kernel of Φ's cardinality, the isogeny is referred to as separable. An m −isogeny is an isogeny having a degree of m. In this article, unless explicitly stated, m -isogeny implies separable.

If an isogeny $\widehat{\Phi}: E_2 \to E_1$ exist such that for every isogeny $\Phi: E_1 \to E_2$.

$$\Phi \circ \widehat{\Phi} = [\deg \Phi]$$

The symbol for the dual isogeny is $\widehat{\Phi}$, and it establishes an equivalence relation between isogenies. $E_1(K)$and $E_2(K)$ have identical numbers of elements if and only if E_1 and E_2 are isogenous over K. If a degree-one isogeny Φ is separable, then it is an isomorphism. The j-invariant characterizes a binary class of elliptic curves that possess a unique isomorphism. If and only if the j −invariant values of two elliptic type curves are same, they are said to be isomorphic over K.

In addition, the length of the kernel of an isogeny is non-infinite. When a finite subset(subgroup) G of E is defined, an elliptic curve $E' = E/G$ and a separable isogeny $\Phi: E \to E'$ with $ker\ \Phi = G$ are produced. There are two techniques for creating isogenies between elliptic curves. Using a specific shape of the elliptic curve and a finite collection of subgroups relating to the kernel, accurate formulae for creating an isogeny provided by Velu.

Subsequently, Kohel [36] suggested using the kernel polynomial for computing isogenies. This work focuses primarily on Velu's formula for computing isogenies, which is based on the transformation described in Velu's methods.

$$(r_P, s_P) \to \left(r_P + \sum_{Q\in G\setminus\{\dot{O}\}}\left(r_{P+Q} - r_Q\right), s_P + \sum_{Q\in G\setminus\{\dot{O}\}}\left(s_{P+Q} - s_Q\right)\right) \quad (18)$$

The translation of the equation by the points in the kernel G has no effect on the equation itself. It is possible to partition a finite subgroup G into two independent sets $G^+ \; and \; G^-$, such that $G\setminus\{\dot{O}\} = G^+ \cup G^-$ and $Q \in G^+ if \; and \; only \; if - Q \in G^-$, For every $Q = (r_Q,\ s_Q) \in G$, the Kohel [37] defined the following terms:

$$g_Q^r = 3r_Q^2 + a,\ g_Q^s = -2s_Q \quad (19)$$

$$v_Q = 2g_Q^r,\ u_Q = \left(g_Q^s\right)^2 \quad (20)$$

$$v = \sum_{Q\in G^+} v_Q,\ \ w = \sum_{Q\in G^+} u_Q + r_Q v_Q \quad (21)$$

Using Eqs. (19), (20), and (21) isogeny is given by

$$\Phi(r,s) \to \left(r + \sum_{Q\in G^+}\frac{v_Q}{r-r_Q} - \frac{u_Q}{(r-r_Q)^2}, s - \sum_{Q\in G^+}\frac{2u_Q s}{(s-s_Q)^3} + v_Q\frac{s-s_Q-g_Q^r g_Q^s}{(r-r_Q)^2}\right) \quad (22)$$

The isogeny order equals with the order of the subgroup G'. Following is an expression for the image curve equation:

$$E': s^2 = r^3 + (\alpha - 5v)r + (\beta - 7w) \quad (23)$$

2.4 Velu's formula for $M_{A,B}$

In this subsection, we discuss the use of Montgomery curves for generating isogenies of equal degrees. Jao and De Feo initially proposed this method, and then Costello et al. [4] refined it. In this work, we show a method to derive a four-isogeny from projective coordinates. Allow $M_{A,B}$ to be a Montgomery curve defined over a quadric extension, with order 2 point $P_2 = (0,0)$ and order 4 point $P_4 = (1, \sqrt{(A + 2/B)})$, for example, $[2]P_4 = P_2$. We characterize the isogeny of degree 2, which maps $P_4$to $(0, 0)$.

$$\Phi: M_{A,B} \to F$$

$$(R:S:T) \to (R(R-T)^2 : S(R^2 - T^2) : R^2T) \quad (24)$$

where $r = \frac{R}{T}\ and\ s = \frac{S}{T}$ for $(r,s) \in M_{A,B}$. The given corresponding image curve is

$$F: Bs^2 = r^3 + (A+6)r^2 + 4(2+A)r \quad (25)$$

To transform the imaged curve back to Montgomery form, it is essential to compute square roots. To address this issue, one can utilize the isogeny ψ, which has a kernel $\langle(0,0)\rangle$.

$$\psi: \mathrm{F} \to M_{A',B'}$$
$$(R:S:T) \to (R', S', T') \quad (26)$$

In the Eq. (25), where $R' = -R(AT + R + 2T)(R + 4T), S' = S(4AT^2 - R^2 + 8T^2)$, and $T' = (A-2)R^2T$. Here, in the form of Montgomery curves, is the equation for the image curve:

$$M_{A',B'}: \frac{B}{(2-A)}s^2 = r^3 - 2\frac{A+6}{(2-A)}r^2 + r \quad (27)$$

We can compute a degree four isogeny $\Phi_1 = \psi \circ \Phi$ from $M_{A,B}$ to $M_{A',B'} = M_{A,B}/\langle P_4\rangle$, but we cannot simply apply this formula twice. To obtain a degree 4^2 isogeny, we cannot simply apply the formula for computing the degree 4 isogeny twice. Instead, an isomorphism of Montgomery curves that assigns the four-torsion point to a fixed point in space is required in conjunction with the degree-4 isogeny. This allows us to apply the four-isogeny recursively to obtain a $4m$-isogeny. The reason for this is that the formula for computing Φ depends on the choice of the point P_4, which has a specific form. Specifically, given a Four-order point $P \neq \pm P_4$ on the Montgomery curve $M_{A,B}$, let $P = (R_M:S_M:T_M)$ and $[2]P = (R_0:S_0:T_0)$ be the projective coordinates of P and $[2]P$, respectively. To accomplish this, we can use an isomorphism ι that maps $[2]P$ to (0,0) and P to the point of a certain form (1, ...).

$$\iota:\ M_{A,B} \to E$$
$$(R:S:T) \to \left(T_M(RT_0 - TR_0) : ST_MT_0 : T(R_MT_0 - T_MR_0)\right) \quad (29)$$

The corresponding equation for the curve is given below:

$$E: \frac{BT_MT_0}{R_MT_0 - T_MR_0}s^2 = r^3 + \frac{T_M(3R_0 + AT_0)}{R_MT_0 - T_MR_0}r^2 + r \quad (30)$$

Four-isogenies can be computed iteratively by combining Φ_1 and ι.

2.5 Velu's formula for $H_{a,b}$

There exist birational maps that convert the Huff curve $H_{a,b}$ to Weierstrass curves. ψ represents the mapping from the function $H_{a,b}$ to the weierstrass curve W. Similarly, demonstrates the isogeny between curves W and W' is shown by Φ. ψ^{-1} shows a Weierstrass curve W transformed into a $H_{a,b}$ curve. Combining these maps allows one to determine the isogeny between Huff curves. The process of transforming Weierstrass curves into Huff curves can be tricky if the final curve takes on a complex shape.

$$s^2 = r^3 + (a+b)r^2 + abr \tag{31}$$

Moody and Shumow [38] first presented the formula for finding the isogeny of two Huff curves with a kernel size of odd length. On Huff curves, the isogeny of order '$m = 2s_1 + 1$' may be computed using the following theorem:

Theorem [38]**.** Assume G is a finite subgroup of the Huff curves $H_{a,b}$ with an odd number of elements '$m = 2s + 1$'and set of points $G = \{(0,1), (\alpha_1, \beta_1), (-\alpha_1, -\beta_1) \dots\dots, (\alpha_s, \beta_s)\}$. Then a normalized m-isogeny from $H_{a,b}$ to $H_{\hat{a},\hat{b}}$, where $\hat{a} = a^{\ell}B^4$ and $\hat{b} = b^{\ell}A^4$, with $A = \prod_{i=1}^{s} \alpha_i$, $B = \prod_{i=1}^{s} \beta_i$, is given by

$$\Psi(r,s) = \left(r\prod_{i=1}^{s}\frac{r^2-{\alpha_i}^2}{{\alpha_i}^2(1-b^2{\alpha_i}^2r^2)}, s\prod_{i=1}^{s}\frac{s^2-{\beta_i}^2}{{\beta_i}^2(1-a^2{\beta_i}^2s^2)}\right) \tag{32}$$

The idea behind the above formula was influenced by the observation that the mapping:

$$(r_P, s_P) \mapsto \left(r_P\prod_{Q\neq(0,0)\in F}\frac{r_{P+Q}}{r_Q}, s_P\prod_{Q\neq(0,0)\in F}\frac{s_{P+Q}}{s_Q}\right) \tag{33}$$

It is important to note that this theory doesn't cover even-degree isogenies.

3. The proposed Huff curve isogeny calculations

On Huff curves, which are frequently used in IBC, we provide optimized formulae for 2-, 3-isogeny, and 4-isogeny. An affine-to-projective transformation is used for the 2- and 3-isogeny formulae to improve their performance. Inspired by the work of Moody and Shumow [38], our approach employs a bi-rational mapping between $H_{a,b}$ and $M_{A,B}$ to produce more accurate equations for calculating even-degree isogenies. In addition, the 4-isogeny formula for $H_{a,b}$ has been obtained by combine the isogeny formula for Montgomery curves with the birational map between $H_{a,b}$ and $M_{A,B}$.

3.1 Two-isogeny on $H_{a,b}$

Suppose there is a two-torsion point $P = (\alpha, \beta)$ on the Huff curve $H_{a,b}$. Let Φ be a two-isogeny with kernel $\langle P \rangle$, which transforms $H_{a,b}$ to the Huff curve $H_{a',b'}$ where $H_{a',b'} = H_{a,b}/\langle P \rangle$. For this isogeny, Moody and Shumow [38] established the formula. Using this formula, we can express Φ as:

Given the curve parameter a' and b' is

$$a' = -(a + 2\eta + b)$$
$$b' = -(a - 2\eta + b)$$

where $\eta^2 = ab$, to prevent inversions from occurring, we compute isogenies between Huff curves on the projective plane rather than the affine plane. Using projective coefficients for the values of $r = \frac{R}{T}, y = \frac{S}{T}$, and curve coefficients $a = \frac{A}{C}, b = \frac{B}{C}$. The following formula for the Two-isogeny is obtained by converting the curve from affine to projective form using projective curve coefficients and projective coordinates:

$$(R' : S' : T') = \Big((BR - AS)\big((BR - AS) + \sqrt{AB}(R - S)\big)^2 : (BR - AS)\big((BR - AS) - \sqrt{AB}(R - S)\big)^2 : (B - A)^2(BR^2 - AS^2)\Big) \tag{34}$$

and,

$$(A' : B' : C') = \big(-\big(A + 2\sqrt{AB} + B\big) : -\big(A - 2\sqrt{AB} + B\big) : C\big)$$

3.2 Three-isogeny for $H_{a,b}$

A Three-torsion point $P = (\alpha, \beta)$ is assumed to be on $H_{a,b}$. Let Φ be a three-isogeny with kernel $\langle P \rangle$, which transforms $H_{a,b}$ to the Huff curve $H_{a',b'}$ where $H_{a',b'} = H_{a,b}/\langle P \rangle$. According to the isogeny formula introduced in Moody and Shumow [39], Φ is given by:

$$\phi(r,s) = \left(r\frac{r^2-\alpha^2}{\alpha^2(1-b^2\alpha^2r^2)}, s\frac{s^2-\beta^2}{\beta^2(1-a^2\beta^2s^2)}\right) \tag{35}$$

And curve parameter a' and b' is

$$\Phi(r,s) = \left(\frac{(br-as)}{(b-a)^2}\frac{((br-as)+\eta(r-s))^2}{br^2-as^2}, \frac{(br-as)}{(b-a)^2}\frac{((br-as)-\eta(r-s))^2}{br^2-as^2}\right) \quad (37)$$

$$a' = a^3\beta^4$$
$$b' = b^3\alpha^4$$

Where y-coordinate is

$$s\frac{s^2-\beta^2}{\beta^2(1-a^2\beta^2s^2)}$$

When calculating isogeny and curve coefficients, we used the projective plane rather than the affine plane to prevent inversions. Let $P = (R_3 : S_3 : T_3)$ be the projective representation of point P, with $\alpha = R_3/T_3$ and $\beta = S_3/T_3$ as its only constraint. To illustrate, let $(S' : T')$ corresponds to the $(S : T)$. The 3-isogeny formula may be simplified by rewriting it such that the projective coordinates are in s-coordinate.

$$\frac{S'}{T'} = \frac{ST_3{}^2(S^2T_3{}^2 - S^2T^2)}{TS_3{}^2(T_3{}^2T^2 - a^2S^2S_3{}^2)} \quad (36)$$

There are three infinite points with order 2 in $H_{a,b}$: $(1,0), (0,1)\ and\ (a,b)$. It is well known that (0,0) is the identity element. Isogeny states that the identity point (0,0) of $H_{a,b}$ maps to the identity point (0,0) of $H_{a',b'}$, the point (0,1) of $H_{a,b}$ maps to the point (0,1) of $H_{a',b'}$, and so on. Therefore, we get $a^2 = \frac{2\beta^2-1}{\beta^4}$ and $b^2 = \frac{2\alpha^2-1}{\alpha^4}$, and then we put in a value into Eq. (37), yielding:

$$\frac{S'}{T'} = \frac{S(S^2T_3{}^2 - S_3{}^2T^2)}{T(T_3{}^2S^2 - 2S_3{}^2S^2 + T^2S_3{}^2)} \quad (38)$$

In summary, the projective version of the s-coordinate of the 3-isogeny formula is obtained from the additional input $(S : T)$.

$$(S' : T') = \left(S\left(S^2T_3{}^2 - S_3{}^2T^2\right) : T(T_3{}^2S^2 - 2S_3{}^2S^2 + T^2S_3{}^2)\right) \quad (39)$$

Let's suppose a' and b' as the image curve's curve coefficients. Substitute the values $a^2 = \frac{2\beta^2-1}{\beta^4}$ and $b^2 = \frac{2\alpha^2-1}{\alpha^4}$ into a' and b', respectively.

$$a' = a\frac{2Y_3{}^2 - Z_3{}^2}{Z_3{}^2}$$
$$b' = b\frac{2X_3{}^2 - Z_3{}^2}{Z_3{}^2}$$

To ignore inversion, projective version of a' and b' are

$$A' = A(2S_3{}^2 - T_3{}^2)$$
$$B' = B(2R_3{}^2 - T_3{}^2)$$
$$C' = CT_3{}^2$$

where $a' = A'/C'$ and $b' = B'/C'$ for $a = A/C$ and $b = B/C$.

3.3 Four isogeny on $H_{a,b}$

The first approach makes use of Velu's formula once the Huff curve has been transformed into its equivalent weierstrass form. However, converting from Weierstrass form to Huff form is not always a straightforward process and may include the use of square roots. Secondly, we may use the birational mapping. Four-isogeny can be computed on a Montgomery curve, and then the curve can be transformed back into a Weierstrass form curve and then into a Huff form curve. To do this, we have followed the steps outlined in [40]. Our chosen composition is briefly described here:

$$H_{a,b} \xrightarrow{\psi} M_{A,B} \xrightarrow{\iota} M_{A',B'} \xrightarrow{\Phi_1} M_{A'',B''} \xrightarrow{\psi'} H_{a',b'} \quad (40)$$

In the Huff curve's projective coordinate form $H_{a,b}$, we take P $(R_4 : S_4 : T_4)$ as a Four-torsion point since Φ_1 is an isogeny identified by Velu and ψ, ψ' are birational mappings. When mapping the Huff curve $H_{a,b}$ to the Montgomery curve $M_{A,B}$, the birational map ψ maps P as follows:

$$\psi(R_4 : S_4) \to (R_M : T_M) = (bR_4 - aS_4 : \sqrt{ab}(S_4 - R_4)) \quad (41)$$

where $A = \frac{a+b}{\sqrt{ab}}$, $B = \frac{1}{\sqrt{ab}}$.

Suppose P' stands in for the effective Four-torsion point on $M_{A,B}$. The idea of the computation with kernel $\langle P' \rangle$ and four-isogeny $\Phi = \Phi_1 \circ \iota$ as stated in [8] and given by

$$(R' : T') = \Big(R\left(2R_MT_MT - R\left(R_M{}^2 + T_M{}^2\right)\right).(R_MT - T_MT)^2 : T(2R_MT_MR - T(R_M{}^2 + T_M{}^2))(T_MR - R_MT)^2\Big) \quad (42)$$

Note that this formula already incorporates the

$$R' = \frac{B\{(A-\sqrt{A^2-4})T(2R_MT_MR-T(R_M{}^2+T_M{}^2))(T_MR-R_MT)^2+2R\left(2R_MT_MT-R(R_M{}^2+T_M{}^2)\right).(R_MR-T_MT)^2\}}{2\sqrt{A^2-4}} \quad (44)$$

$$S' = \frac{B\{(A+\sqrt{A^2-4})T(2R_MT_MR-T(R_M{}^2+T_M{}^2))(T_MR-R_MT)^2+2R\left(2R_MT_MT-R(R_M{}^2+T_M{}^2)\right).(R_MR-T_MT)^2\}}{2\sqrt{A^2-4}} \quad (45)$$

Algorithm 1. Huff curve 3-isogeny determination

Require: Three torsion point $P(R_3:S_3:T_3)$, Curve Co-efficient A, B and a point $Q(S:T)$ on curve on $H_{a,b}$ where $a = \frac{A}{C}$, $b = \frac{B}{C}$.

1: $s_0 \leftarrow (S)^2$ // $s_0 = (S)^2$
2: $s_1 \leftarrow (T)^2$ // $s_1 = (T)^2$
3: $s_2 \leftarrow (R_3)^2$ // $s_2 = (R_3)^2$
4: $s_3 \leftarrow (S_3)^2$ //$s_3 = (S_3)^2$
5: $s_4 \leftarrow (T_3)^2$ // $s_4 = (T_3)^2$
6: $s_5 \leftarrow s_0 \cdot s_4$//$s_5 = S^2{T_3}^2$
7: $s_6 \leftarrow s_3 \cdot s_1$ // $s_6 = T^2{S_3}^2$
8: $s_7 \leftarrow s_0 \cdot s_3$ // $s_7 = S^2{S_3}^2$
9: $S' \leftarrow S \cdot (s_5 - s_6)$ // $S' = S(S^2{T_3}^2 - T^2{S_3}^2)$
10: $T' \leftarrow Z \cdot (s_5 + s_6 - 2s_7)$ // $T' = T(S^2{T_3}^2 + T^2{S_3}^2 - 2S^2{S_3}^2)$
11: $A' \leftarrow A \cdot (2s_3 - s_4)$ // $A' = A(2{S_3}^2 - {T_3}^2)$
12: $B' \leftarrow B \cdot (2s_2 - s_4)$ // $B' = B(2{R_3}^2 - {T_3}^2)$

Table 1. Analyzing the differences in the number of procedures required to create isogenies on different curves

Curves	2-isogeny	3-isogeny
Montgomery [18,19]	$2s_2 + 4m_2 + 5a_2$	$5s_2 + 6m_2 + 14a_2$
Edwards [29,30]	$3s_2 + 31m_2$	$6m_2 + 5s_2 + 11a_2$
Huff (this work)	$2s_2 + 3m_2 + 7a_2$	$5s_2 + 5m_2 + 5a_2$

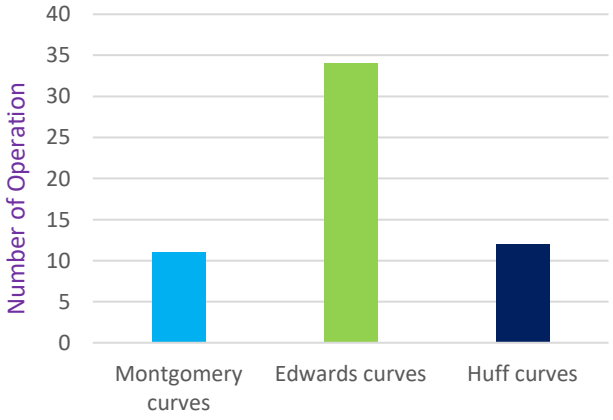

Figure. 1 Analyzing the performance of 2-isogeny in relation to the Montgomery, Edwards, and Huff curves

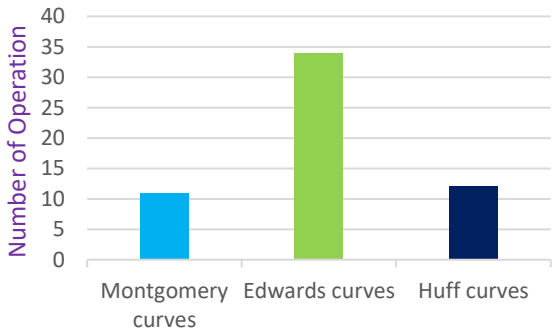

Figure. 2 Analyzing the performance of 3-isogeny in relation to the Montgomery, Edwards, and Huff curves

isomorphism, and thus no further transformation is required. Finally, the mapping from $M_{A'',B''}$ to the $H_{a',b'}$ through birational map ψ' is given as:

$$\psi'(R':T') \longrightarrow (R', S') = \left(\frac{B\{(A-\sqrt{A^2-4})T'+2R'\}}{2\sqrt{A^2-4}}, \frac{B\{(A+\sqrt{A^2-4})T'+2R'\}}{2\sqrt{A^2-4}}\right) \quad (43)$$

Image curve $H_{a',b'}$ has curve coefficients $a'$and b' equal to

$$a' = \frac{A-\sqrt{A^2-4}}{2B}$$
$$b' = \frac{A+\sqrt{A^2-4}}{2B}$$

The combination of the three maps ψ, Φ, and ψ' gives rise to a Four-isogeny from $H_{a,b}$ to $H_{a',b'}$. To obtain the four-isogeny, we computed (R', S') from the input point (R, S) on $H_{a,b}$ using the following equation:

4. Results

In this present work, an approach for quickly calculating the 2, 3, and 4 isogenies on huff curves has been illustrated. We have developed separate algorithms for computing the two-isogenies and three-isogenies. The performance of our algorithms is evaluated using field operations such as addition, multiplication, and squaring. Table 1 displays the performance of our isogeny formulas for the Edward, Montgomery, and Huff curves. In the table, a_2 denotes addition or subtraction, s_2 denotes squaring, and m_2 denotes multiplication. Based on our findings, isogenies defined on Huff curves perform better than those defined on Montgomery and Edwards curves. Since our method relies more on subtraction than field addition, it achieves similar results to Huff curves while reducing the performance gap. Overall, our algorithm presents an efficient approach for computing isogenies on huff curves.

5. Conclusion

In this study, we presented the 2, 3, and 4-Isogeny formula for Huff Curves. It is applicable to IBC. We used the projective coordinates and projective curve coefficients to enhanced the formula for 2- and 3-isogeny. When computing even-degree isogeny, we take advantage of the efficiency by creating a birational mapping between the Huff and Montgomery curves. by integrating the isogeny on Montgomery curves with the birational mapping, 2 and 3-isogeny onto the Huff curve have computational costs of $2s_2 + 3m_2 + 7a_2$ and $5s_2 + 5m_2 + 5a_2$, respectively. Furthermore, we showed that isogenies for Huff curves similarly effective as isogenies for Montgomery curves by putting our theories.

Conflicts of interest

There are no competing interests on the part of the authors, according to the corresponding author.

Author contributions

The paper background work, conceptualization, methodology and implementation have been done by first author. The result analysis and comparison have been done by fourth and fifth author. Preparing and editing draft, visualization have been done by third author. The supervision and review of work has been done by second author.

References

[1] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalili, B. Koziel, B. LaMacchia, P. Longa, and M. Naehrig, "SIKE: Super-singular isogeny key encapsulation", *Submission to the NIST Post-Quantum Standardization Project*, Vol. 152, pp. 154-155, 2017.

[2] J. M. Couveignes, "Hard homogeneous spaces", *Cryptology ePrint Archive*, 2006. https://eprint.iacr.org/2006/291.pdf

[3] A. Stolbunov, "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves", *Advances in Mathematics of Communications*, Vol. 4, No. 2, p. 215, 2010.

[4] S. Jaques and J. M. Schanck, "Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE", In: *Proc. of Annual International Cryptology Conference*, pp. 32-61, 2019, doi: 10.1007/978-3-030-26948-7_2.

[5] A. Childs, D. Jao, and V. Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time", *Journal of Mathematical Cryptology*, Vol. 8, No. 1, pp. 1-29, 2014.

[6] R. Azarderakhsh, B. Koziel, S. H. F. Langroudi, and M. M. Kermani, "Fpga-sidh: High performance implementation of super-singular isogeny diffie-hellman key-exchange protocol on fpga", *Cryptology ePrint Archive*, Vol. 672, pp. 1-18, 2016.

[7] R. Azarderakhsh, B. E. Lang, D. Jao, and B. Koziel, "EdSIDH: Super-singular Isogeny Diffie-Hellman Key Exchange on Edwards Curves", In: *Proc. of International Conference on Security, Privacy, and Applied Cryptography Engineering SPACE*, pp. 125-141, 2018, doi: 10.1007/978-3-030-05072-6_8.

[8] C. Costello, P. Longa, and M. Naehrig, "Efficient algorithms for super-singular isogeny Diffie-Hellman", In: *Proc. of Annual International Cryptology Conference*, pp. 572-601, 2016, doi: 10.1007/978-3-662-53018-4_21.

[9] H. Seo, Z. Liu, P. Longa, and Z. Hu, "SIDH on ARM: faster modular multiplications for faster post-quantum super-singular isogeny key exchange", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2018, No. 3, pp. 1-20, 2018.

[10] L. D. Feo, J. Kieffer, and B. Smith, "Towards practical key exchange from ordinary isogeny graphs", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 365-394, 2018, doi: 10.1007/978-3-030-03332-3_14.

[11] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: an efficient post-quantum commutative group action", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 395-427, 2018, doi: 10.1007/978-3-030-03332-3_15.

[12] W. Beullens, T. Kleinjung, and F. Vercauteren, "CSI-FiSh: efficient isogeny-based signatures through class group computations", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 227-247, 2019, doi: 10.1007/978-3-030-34578-5_9.

[13] C. Costello and H. Hisil, "A simple and compact algorithm for SIDH with arbitrary degree isogenies", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 303-329, 2017, doi: 10.1007/978-3-319-70697-9_11.

[14] D. J. Bernstein, L. D. Feo, A. Leroux, and B. Smith, "Faster computation of isogenies of large prime degree", *Open Book Series*, Vol. 4, No. 1, pp. 39-55, 2020.

[15] C. Costello, "B-SIDH: super-singular isogeny Diffie-Hellman using twisted torsion", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 440-463, 2020, doi: 10.1007/978-3-030-64834-3_15.

[16] J. C. Saab, J. J. C. Domínguez, S. Jaques, and F. R. Henríquez, "The SQALE of CSIDH: Sublinear Vélu Quantum-resistant isogeny Action with Low Exponents", *Journal of Cryptographic Engineering*, pp. 349-368, 2021, doi: 10.1007/s13389-021-00271-w.

[17] A. Canteaut, Y. Ishai, and C. Peikert, "He gives C-sieves on the CSIDH", *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 463-492, 2020, doi: 10.1007/978-3-030-45724-2_16.

[18] C. Costello and B. Smith, "Montgomery curves and their arithmetic", *Journal of Cryptographic Engineering*, Vol. 8, No. 3, pp. 227-240, 2018.

[19] M. Meyer, S. Reith, and F. Campos, "On hybrid SIDH schemes using Edwards and Montgomery curve arithmetic", *Cryptology ePrint Archive*, 2017.

[20] B. H. Im and B. D. Kim, "Ranks of rational points of the Jacobian varieties of hyperelliptic curves", *Journal of Number Theory*, Vol. 195, pp. 23-50, 2019.

[21] A. Dąbrowski and T. Jędrzejak, "Elliptic curves over the rationals with good reduction outside two odd primes", *Journal of Number Theory*, Vol. 202, pp. 254-277, 2019.

[22] M. Meyer and S. Reith, "A faster way to the CSIDH", In: *Proc. of International Conference on Cryptology in India*, pp. 137-152, 2018, doi: 10.1007/978-3-030-05378-9_8

[23] S. Kim, K. Yoon, Y. H. Park, and S. Hong, "Optimized method for computing odd-degree isogenies on Edwards curves", In: *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 273-292, 2019, doi: 10.1007/978-3-030-34621-8_10.

[24] F. L. P. Broon, T. Dang, E. Fouotsa, and D. Moody, "Isogenies on twisted Hessian curves", *Journal of Mathematical Cryptology*, Vol. 15, No. 1, pp. 345-358, 2021.

[25] Y. Huang, Y. Jin, Z. Hu, and F. Zhang, "Optimizing the evaluation of ℓ-isogenous curve for isogeny-based cryptography", *Information Processing Letters*, Vol. 178, 2020, doi: 10.1016/j.ipl.2022.106301.

[26] Z. Hu, Z. Liu, L. Wang, and Z. Zhou, "Simplified isogeny formulas on twisted Jacobi quartic curves", *Finite Fields and Their Applications*, Vol. 78, 2022, doi: 10.1016/j.ffa.2021.101981.

[27] K. Dey, S. K. Debnath, P. Stănică, and V. Srivastava, "A post-quantum signcryption scheme using isogeny based cryptography", *Journal of Information Security and Applications*, Vol. 69, 2022, doi: 10.1016/j.jisa.2022.103280.

[28] Z. Tao, Z. Hu, and Z. Zhou, "Faster isogeny computation on twisted Hessian curves", *Applied Mathematics and Computation*, Vol. 444, 2023, doi: 10.1016/j.amc.2022.127823.

[29] R. Azarderakhsh, E. B. Lang, and D. Jao, and B. Koziel, "EdSIDH: super-singular isogeny Diffie-Hellman key exchange on Edwards curves", In: *Proc. of International Conference on Security, Privacy and Applied Cryptography Engineering*, pp. 125-141, 2018, doi: 10.1007/978-3-030-05072-6_8.

[30] S. Kim, K. Yoon, J. Kwon, S. Hong, and Y. H. Park, "Efficient isogeny computations on twisted Edwards curves", *Security and Communication Networks*, 2018, doi: 10.1155/2018/5747642.

[31] M. Joye, M. Tibouchi, and D. Vergnaud, "Huff's

model for elliptic curves", *International Algorithmic Number Theory Symposium*, pp. 234-250, 2010, doi: 10.1007/978-3-642-14518-6_20.

[32] H. Wu and R. Feng, "Elliptic curves in Huff's model", *Wuhan University Journal of Natural Sciences*, Vol. 17, No. 6, pp. 473-480, 2012.

[33] N. G. Orhon and H. Hisil, "Speeding up Huff form of elliptic curves", *Designs, Codes and Cryptography*, Vol. 86, No. 12, pp. 2807-2823, 2018.

[34] K. Okeya, H. Kurumatani, and K. Sakurai, "Elliptic curves with the Montgomery-form and their cryptographic applications", In: *Proc. of International Workshop on Public Key Cryptography*, pp. 238-257, 2000, doi: 10.1007/978-3-540-46588-1_17

[35] I. E. Shparlinski and A. V. Sutherland, "On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average", *LMS Journal of Computation and Mathematics*, Vol. 18, No. 1, pp. 308-322, 2015.

[36] G. B. Huff, "Diophantine problems in geometry and elliptic ternary forms", *Duke Mathematical Journal*, Vol. 15, No. 2, pp. 443-453, 1948.

[37] D. R. Kohel, "Endomorphism rings of elliptic curves over finite fields", *ProQuest LLC, Ann Arbor, MI*, Thesis (Ph.D.)–University of California, Berkeley, 1996.

[38] D. Moody and D. Shumow, "Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves", *Mathematics of Computation*, Vol. 85, No. 300, pp. 1929-1951, 2016.

[39] L. D. Feo, D. Jao, and J. Plût, "Towards quantum-resistant cryptosystems from super-singular elliptic curve isogenies", *Journal of Mathematical Cryptology*, Vol. 8, No. 3, pp. 209-247, 2014.

[40] J. Renes, "Computing isogenies between Montgomery curves using the action of (0, 0)", In: *Proc. of International Conference on Post-Quantum Cryptography*, pp. 229-247, 2018, doi: 10.1007/978-3-319-79063-3_11.