Properties of Isogeny Graph of Non-Cyclic Edwards Curves

Serhii Abramov[1], Anatoly Bessalov[1], and Volodymyr Sokolov[1]

[1] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

Some properties of isogenies of non-cyclic supersingular Edwards curves, which are used in the implementation of the CSIDH algorithm, are considered. This article continues the consideration of properties using the example of these classes of supersingular Edwards curves from previous work. All isogeny calculations are performed using one parameter of the curve equation d. Isogeny properties are modeled on an isogeny graph and are considered graph properties. Recommendations are given for selecting some cryptosystem parameters. It is shown which parameters d are prohibited for use in CSIDH algorithms and that the transition from one isogeny to another is not always possible.

Keywords

Post-quantum cryptography, commutative supersingular isogeny Diffie-Hellman algorithm, curve in generalized Edwards form, non-cyclic Edwards curve, curve order, point order, graph of isogeny.

1. Introduction

The works [1] present a modification of the CSIDH algorithm, built on isogenies of non-cyclic Supersingular Edwards Curves (SEC) [2–6], instead of traditional curve arithmetic in the Montgomery form. This Post Quantum Cryptography (PQC) algorithm differs from other known algorithms by its minimum key length, which is close to the prime field modulus F_p, on which group operations are performed. An example is given of calculating the parameters of these curves $p = 839$, on the isogenies of which the algorithm is implemented.

This article presents new results of studying isogenies of non-cyclic supersingular Edwards curves using graphs that were also previously used in articles [7–9].

At one of the stages of the algorithm, group operations are performed on l_k-isogeny cycles. The number of steps in operation $[l_k^{e_k}]$ corresponds to the secret exponent of the vector Ωκ = (e_1, e_2, ..., $e_{K, ...}$). Work [10] justified the identification of the curves in generalized Edwards form by one parameter *d*. It made it possible to identify quadratic and twisted Edwards curves (non-cyclic Edwards curves) over the field F_p by one parameter d.

The article models the choice of a vector of exponents of a secret key by an isogeny graph [9]. The study of the parameters of isogenic curves continued using the example of 840 order curves.

The work [1] considers an example of constructing isogenies for non-cyclic SEC with parameters $(a = \pm 1)$, $p = 839$, $N_E = 840$ (66 curves). There are values of 66 parameters d for all 66 curves and provides calculations of isogenies of degrees 3, 5, and 7 for 33 curves in that work. It is shown that the choice of some curves is unsuccessful (curve with d=733). This article shows which other d parameters are prohibited. In addition, it is shown that the transition from one isogeny to another is not always possible.

2. Theoretical Foundation

The PQC CSIDH (Commutative SIDH) algorithm was proposed by the authors of [9] to solve the key exchange problem (SIDH-

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: s.abramov@kubg.edu.ua (S. Abramov); a.bessalov@kubg.edu.ua (A. Bessalov); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0002-5145-2782 (S. Abramov); 0000-0002-6967-5001 (A. Bessalov); 0000-0002-9349-7946 (V. Sokolov)

Supersingular Isogeny Diffie-Hellman [10]), based on isogenic mappings of elliptic curves in general as additive Abelian groups [11–13]. Such a display over a simple field F_p is defined as the class group action and is commutative. In comparison with the known original circuit CRS [14] on non-supersingular curves, the use of isogenies of supersingular curves made it possible to speed up the algorithm and obtain the smallest known key size (512 bits per [9, 15]).

Let the curve E order N_E contains points of small odd orders $l_k, k=1,2,...,K$. Then there is an isogenic curve E' same order N_E.

In the algorithm, repeating this operation e_k times denoted by $[l_k^{e_k}]*E$. Isogeny exponent values $e_k \in Z$ determine the length of the chain of isogenies of degree l_k. In [12], the range of exponent values was adopted $[-m \le e_k \le m], m=5,\ K=74,$ which provides a 128-bit security level against quantum computer attacks. Negative values of the exponent mean a transition to a supersingular quadratic torsion curve [1].

Non-interactive Diffie-Hellman key exchange involves three stages [9]. The second stage is the Calculation of public keys. Each participant using his secret key $\Omega_A = (e_1, e_2, .., e_K)$ builds an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ and calculates the curve $E_A = \Theta_A * E_0$. For each l_i is calculated exactly e_i isogeny.

In [11] the mapping formulas $\phi(P)$ are given for SEC, depending on two parameters a and d. It shows that $\phi(x,y)$ is l-isogeny from the curve $E_{a,d}$ into a curve $E_{a',d''}$ with parameters:

$$a' = a^l,\ d' = d^l A^8,$$
$$A = \prod_{i=1}^{s} \alpha_i, \qquad (1)$$

The parameter d uniquely defines the curve. We will use (1) to calculate the parameters of the chain of isogenies.

In [1] the implementation of the CSIDH algorithm on quadratic and twisted (SECs), forming quadratic torsion pairs with the same order is considered. Such curves exist only when $p \equiv -1 \bmod 8$ and have order $N_E = N_E^t = p+1 = cn\ (n-odd), c \equiv 0 \bmod 8$. Let such a pair of curves contain kernels of the 3rd, 5th, and 7th orders with the value $n=105$, then the minimum prime $p = 8m-1 = 839$ and the order of these curves $N_E = 8n = 840$. The parameter *d* of the entire family made 418 quadratic Edwards curves. This parameter is equal squares $d = r^2 \bmod p, \dots r = 2 \dots 419$. From these 66 pairs of quadratic and twisted SECs with parameters [1] $a = \pm 1$ и $\chi(ad) = 1$ were found.

For the first curve $E_d^{(0)} = E_{144}$ in [1], 3-, 5- and 7-isogenies were constructed and the parameters $d^{(i)}$ of isogenic chains of curves $E_d^{(i)}, i = 0,1,2,...,T$ were found. Curve E144 gives rise to a chain of isogenies of degree 3 with a period of 33. It includes half of all curves of order 840. Let's call them the first segment of curves. Chains 5 and 7 of isogenies also consist of these same curves.

3. Isogeny Graph

Fig. 1 shows the graph of these isogenies of the first segment. The graph shows one chain of 3-isogenies, where the values of the parameter d of the isogenic curves are shown inside the yellow, green, and gray rectangles. The chain starts from curve d=144 and the next calculated isogeny is located clockwise.

Isogenies of degrees 5 and 7 form two chains of each degree (two pairs). In Fig. 1, chains of isogenies of degree 5 are indicated by solid arrows and degrees 7 by dotted arrows. The first chain of each pair contains identical curves from 1/3 of all curves, i.e. have a period of 11 (in Fig. 1a they are indicated in yellow). The second of each pair of chains contains curves from the second one-third of all curves (indicated in green in Fig. 1b). And one-third does not have isogenies 5 and 7 degrees (empty points of the graph are indicated in gray).

In addition to the above, this work also presents isogeny graphs containing the second half of 66 curves of order 840 (second segment) Fig. 2. They also form a chain of 3-isogenies with a period of 33 and a pair of chains of 5 and 7 isogenies with a period of 11.

The first curves are marked in yellow. The second curve is marked in green. In the chain of 3-isogenies, the starting point was the point d = 784 from Table 1 [1] (Fig. 2).

The structure of all isogenies of Edwards supersingular curves is presented in Fig. 3. All curves form two non-intersecting segments of 33 curves in every. The curves of each segment form one chain of isogenies of degree 3 (period 33) and a pair of chains of degrees 5 and 7. A total of 2 chains of 3-isogenies, 4 chains of 11 order isogenies of degree 5, and 4 chains of 11 order isogenies of degree 7.

Table 1 shows some of the points of each segment and which chains of isogenies of degrees 5 and 7 these points are included in.

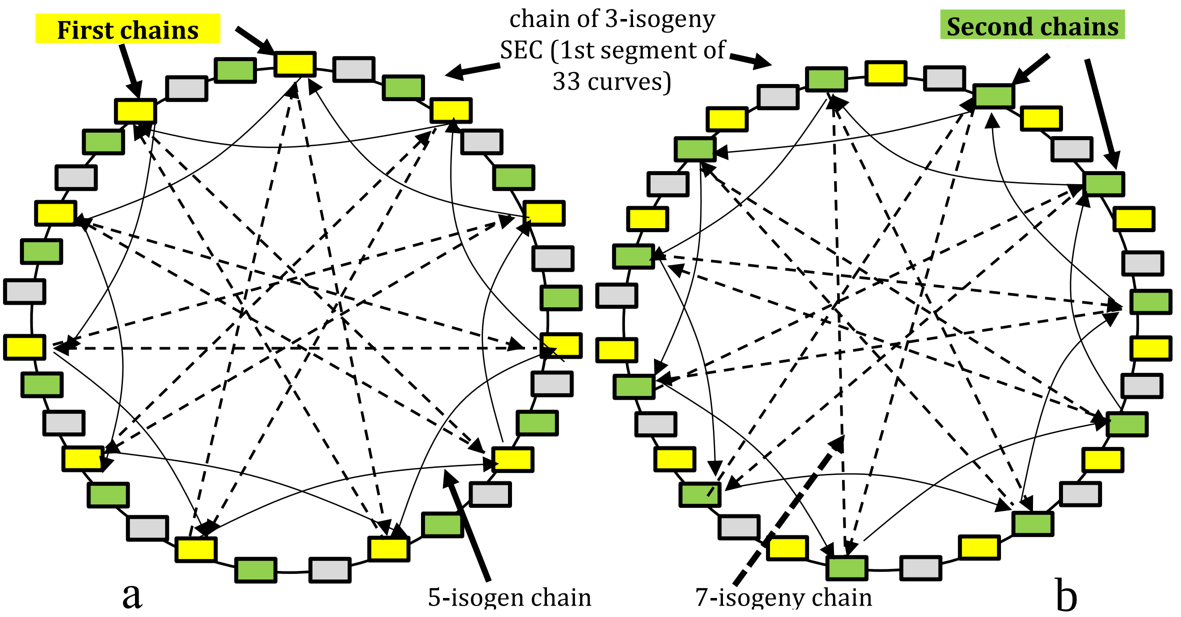


Figure 1: Isogeny graph of the first segment: (a) only the first chains of isogenies of degrees 5 and 7 are shown, and (b) only the second chains of isogenies of degrees 5 and 7 are shown.

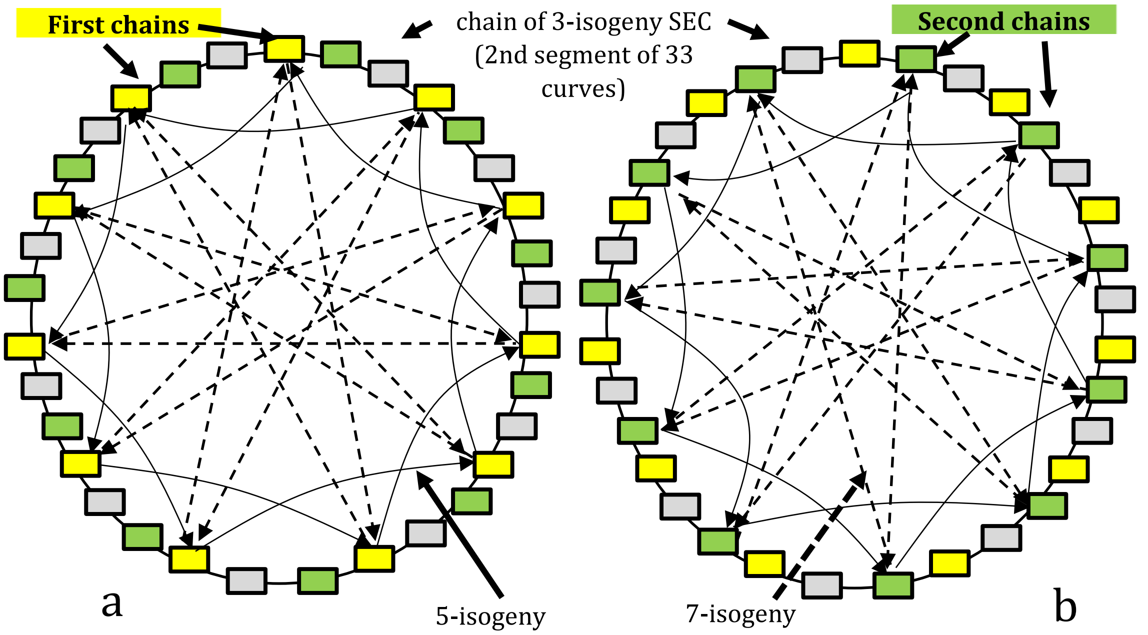


Figure 2: Graph of isogenies of the second segment: (a) only the first chains of isogenies of degrees 5 and 7 are shown, and (b) only the second chains of isogenies of degrees 5 and 7 are shown.

Make a transition between chains of isogenies of degrees 5 and 7 (in both directions) only if their numbers in the pair match (i.e. within the same color of yellow or green in Fig. 1 and Fig. 2). You can also switch to the chain of 3-isogenies at any step, and from the chain of 3-isogenies you can get to the chains of 5 and 7 isogenies only at 11 points of the chain of 3-isogenies. In the first segment, you can go to the first chain of 5 and 7 isogenies only from yellow points 144, 76,258, 293, 243, 2, 788, 636, 112, 182, 752, and to the second chain from green points. And accordingly for the second segment.

The graph shows that the exponent in the vector $\Omega_K = (e_1, e_2, ..., e_K)$ corresponding to isogeny l_3 *3* degrees must be a multiple of 3. Only after every 3 steps, you can get to points coinciding with the graph of 5 or 7 isogenies.

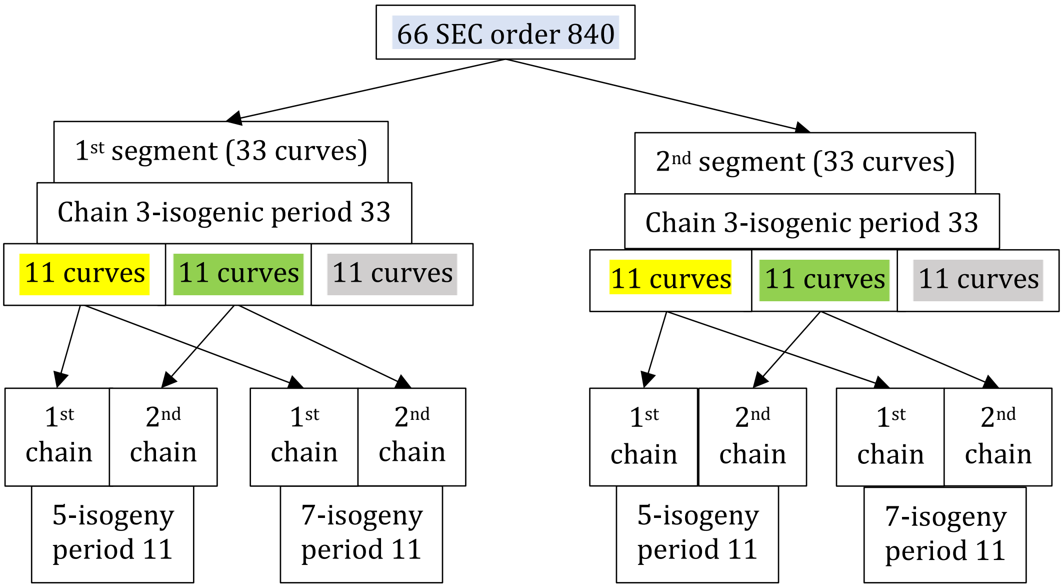


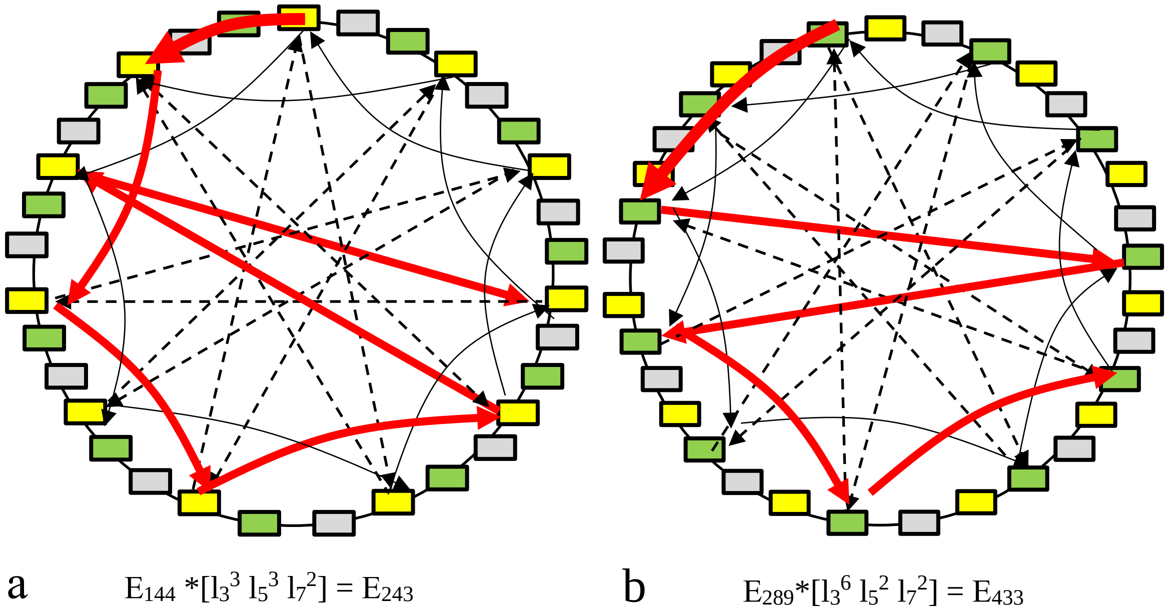
Figure 3: Structure of SEC isogenies of the 840th order

Table 1
Parameters d of all curves of order 840.

Isogeny	№chain	1	2	3	4	5	6	...	33	
3-isogenies (1st segment)	1	144	414	405	2	28	259	...	289	Fig. 1
3-isogenies (2nd segment)	1	90	705	610	810	420			784	Fig. 2
5-isogeny	1	Yes	—	—	Yes	—	—		—	Fig. 1a, 2a
5-isogeny	2	—	—	Yes	—	—	Yes		Yes	Fig.1b, 2b
7-isogeny	1	Yes	—	—	Yes	—	—		—	Fig.1a, 2a
7-isogeny	2	—	—	Yes	—	—	Yes		Yes	Fig.1b, 2b

Fig. 4 shows examples of graph transitions for group operations a) E_{144} *$[l_3^3\ l_5^3\ l_7^2] = E_{243}$ and b) E_{289}*$[l_3^6\ l_5^2\ l_7^2] = E_{433}$.

Transitions are carried out between isogenies with parameters: d = 144->243 and d = 144->243.



a $E_{144} *[l_3^{3}\, l_5^{3}\, l_7^{2}] = E_{243}$ b $E_{289}*[l_3^{6}\, l_5^{2}\, l_7^{2}] = E_{433}$

Figure 4: Examples of graph transitions. Transitions are carried out between isogenies with parameters: d = 144->243 and d = 289->433

The figure shows that the number of steps along the chain of 3-isogenies is always a multiple of 3. Otherwise, it is impossible to get to the chains of isogenies of degrees 5 and 7. The figure shows steps 3 and 6 along the chain of 3-isogenies.

4. Conclusion

The graph (Fig. 1 and 2) is not fully connected and therefore not all paths between vertices are accessible.

It is not possible to move from a chain of 3-isogenies to the rest at an arbitrary point in the graph. You need to choose steps in the 3-isogeny chain not arbitrarily, but so as not to end up in empty points of the graph.

The first and second (yellow and green) chains of each pair do not have common curves (common points of the graph), so a direct transition between them is not possible. This transition can be made by returning to the 3rd order chain and passing along several steps so as not to end up in an empty (gray) point. The transition between segments is generally impossible because the corresponding graphs do not have common points.

Such properties of the isogeny graph somewhat limit the freedom of wandering around the graph and the number of paths between curves is reduced by approximately half, and this must be taken into account when implementing the CSIDH algorithm. It should be noted that given the huge number of isogenies in real systems, these restrictions have virtually no effect on the security of the cryptosystem.

References

[1] A. Bessalov, L. Kovalchuk, S. Abramov, Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves, Cybersecur. Educ. Sci. Tech. 1(17) 2022 128–144. doi:10.28925/2663-4023.2022.17.128144.

[2] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[3] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

[4] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and

Telecommunication Systems, vol. 3288 (2022) 1–10.

[5] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[6] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 1–13.

[7] A. Rostovtsev, A. Stolbunov. Public-Key Cryptosystem Based on Isogenies, Cryptol. ePrint Arch. (2006).

[8] A. Bessalov, Elliptic Curves in Edwards form and Cryptography, Monograph, Kyiv (2017).

[9] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication System, vol. 2923 (2021) 1–11.

[10] D. Bernstein, et al., Quantum Circuits for the CSIDH: Optimizing Quantum Evaluation of Isogenies, Annual International Conference on the Theory and Applications of Cryptographic Techniques (2019) 409–441. doi: 10.1007/978-3-030-17656-3_15.

[11] L. De Feo, D. Jao, J. Plût, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, J. Math. Cryptol. 8(3) (2014) 209–247. doi:10.1515/jmc-2012-0015.

[12] W. Castryck, et al., CSIDH: An Efficient Post-Quantum Commutative Group Action, International Conference on the Theory and Application of Cryptology and Information Security (2018) 395–427. doi:10.1007/978-3-030-03332-3_15.

[13] W. Diffie, M. Hellman, New Directions in Cryptography, Democr. Cryptogr. 22(6) (1976) 644–654. doi:10.1145 /3549993.3550007.

[14] A. Rostovtsev, A. Stolbunov. Public-Key Cryptosystem Based on Isogenies, Cryptol. ePrint Arch. (2006).

[15] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves, in: 2nd International Workshop on Modern Machine Learning Technologies and Data Science I, vol. 2631 (2020) 30–39.