SIDH with masked torsion point images

(Preliminary version)

Tako Boris Fouotsa

LASEC-EPFL, Switzerland
tako.fouotsa@epfl.ch

Abstract. We propose a countermeasure to the Castryck-Decru attack on SIDH. The attack heavily relies on the images of torsion points. The main input to our countermeasure consists in masking the torsion point images in SIDH in a way they are not exploitable in the attack, but can be used to complete the key exchange. This comes with a change in the form the field characteristic and a considerable increase in the parameter sizes.

Keywords: Post-quantum cryptography · supersingular isogenies · SIDH · SIKE · torsion point attacks

Note. This note has been extended and merged with [10] in [5]. After a rigorous security analysis, the sizes of the parameters were increased. Please check [5] for the updates.

1 Introduction

SIDH [8,4] and SIKE [7] are two of the most important schemes in isogeny-based Cryptography. Up to 2021, the main (passive) cryptanalysis results on SIDH/SIKE were Petit's torsion point attacks [12] and their improvements [3]. About two weeks ago, Castryck and Decru [1] described a devastating attack on SIDH that recovers the secret key in SIDH and SIKE, instantiated with the NIST parameters, in few hours. There are various follow-up speedups [11] by other authors that run in minutes or seconds. The attack exploits the availability of the endomorphism ring of the starting curve E_0, the torsion point information and the knowledge of the degree of the secret isogeny. Assuming that the endomorphism ring of the starting curve E_0 is not provided, a concurrent work by Maino and Martindale [9] uses similar ideas to show that the SIDH/SIKE parameters still fall short respect to the various security levels they were suggested for. Few days later, Damien Robert [13] extended this same ideas to get a polynomial time attack even when the endomorphism ring of the starting curve E_0 is unknown.

Contributions. In this note, we present a high level description of a countermeasure to the Thomas-Decru attack (and extensions by Maino-Martindale and Damien Robert). Our main input is to hide (up to some extend) the torsion point images from a malicious adversary. To do so, we scale the torsion point images by a random uniformly sampled integer. This does not affect the underlying SIDH key exchange, but prevents adversaries from running the Castryck-Decru attack.

2 Masking torsion point images

We refer to[2,9,13] for details about the Castryck-Decru attack and improvements. The latest version of the attack requires two main ingredients:

1. the degree A of the secret supersingular isogeny $\phi : E_0 \to E$;
2. the images $\phi(P)$, $\phi(Q)$ of a torsion basis (P, Q) of the B-torsion $E_0[B]$ where B is an integer coprime to A such that $B > A$.

Our aim is to instantiate SIDH such that the direct images $\phi(P)$, $\phi(Q)$ of P and Q are not available to adversaries, but the key exchange still succeeds: this means that when given a point $R \in E_0[B]$, one should be able to compute a generator of the group $\phi(\langle R \rangle)$.

Remark 1. Let $\phi : E_0 \to E$ be an isogeny of degree A. Let B be an integer coprime to A, set $E_0[B] = \langle P, Q \rangle$. Then

$$e_B(\phi(P), \phi(Q)) = e_B(P, Q)^A$$

where $e_B(\cdot, \cdot)$ is the Weil pairing. Moreover, if B is smooth, then when given $\phi(P)$ and $\phi(Q)$, one can recover $A = \deg \phi$ by solving a discrete logarithm problem between $e_B(\phi(P), \phi(Q))$ and $e_B(P, Q)$. In the whole of this note, the isogeny degrees and torsion point orders are always smooth.

To achieve our goal, we scale the images $\phi(P)$, $\phi(Q)$ of P and Q of P and Q by a random uniformly sampled integer $a \in \mathbb{Z}/B\mathbb{Z}^\times$. That is instead of revealing $\phi(P)$, $\phi(Q)$, one reveals $[a]\phi(P)$, $[a]\phi(Q)$. We claim that this suffices (modulo some adjustments of the public parameters).

- The underlying SIDH key exchange succeeds: given $R = [x]P + [y]Q$, then $\langle [x]([a]\phi(P)) + [y]([a]\phi(Q)) \rangle = \langle [a]\phi([x]P + [y]Q) \rangle = \langle [a]\phi(R) \rangle = \langle \phi(R) \rangle$ because $a \in \mathbb{Z}/B\mathbb{Z}^\times$. Hence Alice and Bob can push their kernels through the other party's isogeny successfully.
- To run the Castryck-Decru in this setting, one can either consider the isogeny ϕ or the isogeny $\psi = [a] \circ \phi$ as the target isogeny in the attack. In the second case, the degree of ψ is $d = a^2 \deg \phi = Aa^2$. Since a was sampled from $\mathbb{Z}/B\mathbb{Z}^\times$, then $a \approx B$, hence $d \approx AB^2$. But then the Castryck-Decru attack is not efficient because $\frac{B}{d} \approx \frac{1}{AB} = \text{negl}$ while the attack requires $B > d$. In the first case, one can assume that condition $B > A$ is satisfied. Then, to the best of our knowledge, one needs to recover the exact images $\phi(P)$, $\phi(Q)$ of P and Q from $[a]\phi(P)$ and $[a]\phi(Q)$ before applying the attack. Pairing computation and discrete logarithm computation in groups of smooth order can be used to recover $a^2 \mod B$. For the scheme to be secure, one needs that from

the knowledge of $a^2 \mod B$, an adversary should not be able to recover $a \mod B$. For this, we set B to have at least λ (λ being the security parameter) distinct prime factors such that an exhaustive search of the integer a in the set of all possible square roots of $a^2 \mod B$ should cost $O(2^\lambda)$. Note that if the wrong square root a_0 is used, then when scaling $[a]\phi(P)$ and $[a]\phi(Q)$ by a_0^{-1}, one gets $[aa_0^{-1}]\phi(P)$ and $[aa_0^{-1}]\phi(Q)$ with $aa_0^{-1} \neq \pm 1 \mod b$. For the Castryck-Decru attack to be successful, there should exist an isogeny $\phi' : E_0 \to E$ of degree A such that $\phi'(P) = [aa_0^{-1}]\phi(P)$ and $\phi'(Q) = [aa_0^{-1}]\phi(Q)$. But since $A \approx B \approx \sqrt{p}$, then this happens with negligible probability.

With respect to the previous discussion, we suggest the following variant of SIDH, that we name M-SIDH: Masked torsion points SIDH).

Setup. Let λ be the security parameter. Let $p = ABf - 1$ be a prime such that $A = \prod_{i=1}^{\lambda} \ell_i$ and $B = \prod_{i=1}^{\lambda} q_i$ are coprime integers, ℓ_i, q_i are distinct small primes, $A \approx B \approx \sqrt{p}$ and f is a small cofactor. Let E_0 be a supersingular curve defined over $\mathbb{F}_{p^2}$. Set $E_0[A] = \langle P_A, Q_A \rangle$ and $E_0[B] = \langle P_B, Q_B \rangle$. The public parameters are E_0, p, A, B, P_A, Q_A, P_B, Q_B.

KeyGeneration. Alice samples uniformly at random two integer a and α from $\mathbb{Z}/B\mathbb{Z}^\times$ and $\mathbb{Z}/A\mathbb{Z}$ respectively. She computes the cyclic isogeny $\phi_A : E_0 \to E_A = E_0/\langle P_A + [\alpha]Q_A \rangle$. Her public key is the tuple $\mathsf{pk}_A = (E_A, [a]\phi_A(P_B), [a]\phi_A(Q_B))$ and her secret key is $\mathsf{sk}_A = \alpha$. The integer a is deleted. Analogously, Bob samples uniformly at random two integer b and β from $\mathbb{Z}/A\mathbb{Z}^\times$ and $\mathbb{Z}/B\mathbb{Z}$ respectively. His public key is $\mathsf{pk}_B = (E_B, [b]\phi_B(P_A), [b]\phi_B(Q_A))$ where $\phi_B : E_0 \to E_B = E_0/\langle P_B + [\beta]Q_B \rangle$ and his secret key is $\mathsf{sk}_B = \beta$. The integer b is deleted.

KeyExchange. Upon receiving Bob's public key (E_B, R_a, S_a), Alice checks that $e_A(R_a, S_a) = e_A(P_A, Q_A)^U$ for some U such that $U/B = u^2 \mod A$ (U/B is a square), if not she aborts. She computes the isogeny $\phi'_A : E_B \to E_{BA} = E_B/\langle R_a + [\alpha]S_a \rangle$. Her shared key is $j(E_{BA})$. Similarly, upon receiving (E_A, R_b, S_b), Bob checks that $e_B(R_b, S_b) = e_B(P_B, Q_B)^V$ for some V such that $V/A = v^2 \mod B$ (V/A is a square), if not he aborts. He computes the isogeny $\phi'_B : E_A \to E_{AB} = E_A/\langle R_b + [\beta]S_b \rangle$. His shared key is $j(E_{AB})$.

Parameters. For the 128 and 192 bits security levels, Table 1 presents the key sizes: secret key, public key and compressed public key. The suggested primes for M-SIDH are

$$p_{128} = 2^2 \cdot \ell_1 \cdots \ell_{256} \cdot 59 - 1$$

and

$$p_{192} = 2^2 \cdot \ell_1 \cdots \ell_{384} \cdot 102 - 1$$

respectively; where ℓ_i is the ith odd prime. Alice uses $A = \ell_1 \cdot \ell_3 \cdots \ell_{2\lambda-1}$ and Bob uses $B = \ell_2 \cdot \ell_4 \cdots \ell_{2\lambda}$.

λ	p (in bits)	secret key	public key	compressed pk
128	$2,308$	≈ 145 bytes	$\approx 1,734$ bytes	$\approx 1,013$ bytes
192	$3,723$	≈ 233 bytes	$\approx 2,796$ bytes	$\approx 1,631$ bytes

Table 1: Tentative parameters for 128 and 192 bits of security.

Remark 2. The countermeasure in this note was inspired by [6][§3.2, after lemma 1] where Petit's torsion point attacks were being considered and we had the same issue in finding the square root of the scalar a^2 when the image points had been scaled by some integer a. We showed that when it comes to the Petit's torsion point attacks, the attacker does not need to know the exact value of the scalar a. To the best of our knowledge, this does not seems to be the case for the Castryck-Decru attack.

Remark 3. In the merged version of this work and [10] (that will be made public in few weeks, including more details and a further analysis), the integers a and b will not be sampled from $\mathbb{Z}/B\mathbb{Z}^\times$ and $\mathbb{Z}/A\mathbb{Z}^\times$, but from $\mu_2(B)$ and $\mu_2(A)$ respectively, where

$$\mu_2(N) = \{x \in \mathbb{Z}/N\mathbb{Z}^\times | x^2 = 1 \mod N\}$$

is the set of square roots of unity modulo N. This would simplify the respective pairing checks in the key exchange to $e_A(R_a, S_a) = e_A(P_A, Q_A)^B$ and $e_B(R_b, S_b) = e_B(P_B, Q_B)^A$ respectively. Which is exactly the check done in SIDH. In fact, the pairing computation reveals no information about the scalar used in the key generation.

References

1. Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975. (page 1)
2. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 395–427. Springer, 2018. (page 2)
3. Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Improved torsion-point attacks on sidh variants. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 432–470, Cham, 2021. Springer International Publishing. (page 1)
4. Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, 2014. Pagesn 209-247. (page 1)
5. Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. M-SIDH and MD-SIDH: countering SIDH attacks by masking information. Cryptology ePrint Archive, Paper 2023/013, 2023. https://eprint.iacr.org/2023/013. (page 1)

6. Tako Boris Fouotsa and Christophe Petit. A new adaptive attack on sidh. In Steven D. Galbraith, editor, *Topics in Cryptology – CT-RSA 2022*, pages 322–344, Cham, 2022. Springer International Publishing. (page 4)
7. David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Aaron Hutchinson, Amir Jalali, Koray Karabina, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular Isogeny Key Encapsulation, October 1, 2020. https://sike.org/files/SIDH-spec.pdf. (page 1)
8. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. (page 1)
9. Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022. https://eprint.iacr.org/2022/1026. (page 1, 2)
10. Tomoki Moriya. Masked-degree SIDH. Cryptology ePrint Archive, Paper 2022/1019, 2022. https://eprint.iacr.org/2022/1019. (page 1, 4)
11. Rémy Oudompheng. An attack on SIDH with arbitrary starting curve, 2022. https://github.com/jack4818/Castryck-Decru-SageMath. (page 1)
12. Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353. Springer International Publishing, 2017. (page 1)
13. Damien Robert. Breaking SIDH in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022. https://eprint.iacr.org/2022/1038. (page 1, 2)