A new adaptive attack on SIDH

Fouotsa, Tako Boris; Petit, Christophe

DOI:
10.1007/978-3-030-95312-6_14

License:
Other (please specify with Rights Statement)

Document Version
Peer reviewed version

Citation for published version (Harvard):
Fouotsa, TB & Petit, C 2022, A new adaptive attack on SIDH. in SD Galbraith (ed.), Topics in Cryptology – CT-RSA 2022: Cryptographers' Track at the RSA Conference 2022, Virtual Event, March 1–2, 2022, Proceedings. 1 edn, Lecture Notes in Computer Science, vol. 13161, Springer, pp. 322-344, Cryptographers' Track RSA Conference, 7/02/22. https://doi.org/10.1007/978-3-030-95312-6_14

A New Adaptive Attack on SIDH

Tako Boris Fouotsa[1] and Christophe Petit[2,3]

[1] Università Degli Studi Roma Tre, Italy
takoboris.fouotsa@uniroma3.it
[2] Université Libre de Bruxelles, Belgium
[3] University of Birmingham's School of Computer Science, UK
christophe.f.petit@gmail.com

Abstract. The SIDH key exchange is the main building block of SIKE, the only isogeny based scheme involved in the NIST standardization process. In 2016, Galbraith et al. presented an adaptive attack on SIDH. In this attack, a malicious party manipulates the torsion points in his public key in order to recover an honest party's static secret key, when having access to a key exchange oracle. In 2017, Petit designed a passive attack (which was improved by de Quehen et al. in 2020) that exploits the torsion point information available in SIDH public key to recover the secret isogeny when the endomorphism ring of the starting curve is known.
In this paper, firstly, we generalize the torsion point attacks by de Quehen et al. Secondly, we introduce a new adaptive attack vector on SIDH-type schemes. Our attack uses the access to a key exchange oracle to recover the action of the secret isogeny on larger subgroups. This leads to an unbalanced SIDH instance for which the secret isogeny can be recovered in polynomial time using the generalized torsion point attacks. Our attack is different from the GPST adaptive attack and constitutes a new cryptanalytic tool for isogeny based cryptography. This result proves that the torsion point attacks are relevant to SIDH[4] parameters in an adaptive attack setting. We suggest attack parameters for some SIDH primes and discuss some countermeasures.

Keywords: Post-quantum cryptography · cryptanalysis · adaptive attacks · SIDH.

1 Introduction

The first isogeny-based cryptographic schemes are the CGL (Charles-Goren-Lauter) hash function [5] and the CRS (Couveignes-Rostovtsev-Stolbunov) key exchange [31,10]. The CRS scheme is a Diffie-Hellman type key exchange scheme using ordinary isogenies of elliptic curves. It is vulnerable to a sub-exponential quantum hidden shift like attack [6] and is not practically efficient.

In 2011, Jao and De Feo proposed SIDH [24,15] that uses isogenies of supersingular elliptic curves. SIDH is efficient and it is not vulnerable to the sub-exponential quantum attack presented in [6]. Nevertheless, a recent paper by

[4] Disclaimer: this result is applicable to SIDH-type schemes only, not to SIKE.

Kutas et al. [26] proves that hidden shift like attacks apply to variants of SIDH with considerably overstretched parameters. The problem of computing isogenies between given supersingular elliptic curves is somehow new in cryptography. Its relation with the supersingular endomorphism ring computation problem have been studied in [30,12]. A rigorous proof of the equivalence between the two problems was recently proposed by Wesolowski [38].

Contrarily to the ordinary case where isogenies commute, supersingular isogenies do not commute in general. In order to solve this issue in SIDH, the images of some well-chosen torsion points trough the secret isogeny are computed and included in the public keys. This implies that the hard problem underlying the security of SIDH is different from the general supersingular isogeny problem. Moreover, this torsion points have been used in designing adaptive and passive attacks on SIDH and/or its (unbalanced) variants.

The most relevant adaptive attack (excluding side channel attacks) on SIDH is due to Galbraith, Petit, Shani and Ti (GPST) [20]. They suppose that one honest party Alice uses a static secret key, and the other malicious party Bob performs multiple key exchanges with Alice. The main idea of the attack is that Bob replaces the images of the torsion points in his public key by malicious ones and obtains some information on Alice's static secret isogeny when looking at the obtained shared secret. Repeating this process a polynomial number of times, Bob totally recovers Alice's private key. The pairing-based key validation method present in SIDH does not detect the GPST adaptive attack. In SIKE [23] (Supersingular Isogeny Key Encapsulation), the GPST adaptive attack is avoided by leveraging SIDH with a variant [22] of the Fujisaki-Okamoto transform [17].

The first passive torsion points attacks are due to Petit [29] and were recently improved by de Quehen et al. [11]. These attacks combine the availability of the endomorphism ring of the starting curve E_0 in SIDH and the torsion point information available in SIDH public keys, to compute a suitable endomorphism of Alice's public curve E_A. The secret isogeny is then recovered using the later endomorphism. For sufficiently unbalanced SIDH parameters (the degrees of the secret isogenies of the parties are of different size), the latest version of the attack [11] is more efficient compared to the generic meet in the middle and the van-Oorschot - Wiener (vOW) attack [36]. For balanced parameters (the degrees of the secret isogenies of both parties are approximately of the same size), the quantum version of the attack is as efficient as the best known quantum attacks [11, Figure 1]. Other passive attacks exploiting the availability of torsion points in the public key are described in [16,26].

The improved torsion points attacks do not apply to SIKE and BSIDH [7] parameters since these parameters are balanced. Therefore, one may argue that they are not relevant to SIDH, BSIDH or any other SIDH like schemes using balanced isogenies degrees.

Contributions. The contribution of this paper is twofold.

First, we revisit the torsion point attacks. The torsion point attacks are used to recover a secret isogeny $\phi : E_0 \to E$ of degree N_A when the images of torsion points of order N_B in E_0 are provided. We prove that one can tweak the

algorithm in such a way that it recovers ϕ when only the images of three cyclic disjoint groups $G_1, G_3, G_3 \subset E_0[N_B]$ of order N_B are provided. This constitutes a generalisation of the torsion point attacks and will be useful in the design of our adaptive attack.

Secondly, we design a new adaptive attack on SIDH-types schemes, including BSIDH. Our attack uses torsion point attacks as a subroutine.

Let $\phi_A : E_0 \to E_A$ be Alice's secret static isogeny in an SIDH instance. Let N_A and N_B be the isogeny degrees of Alice and Bob respectively. Our attack actively recovers the images through ϕ_A of three cyclic disjoint groups $G_1, G_3, G_3 \subset E_0[NN_B]$ of order N_BN where N is a well chosen integer coprime to N_A. This leads to an unbalanced SIDH instance for which the torsion point attacks can be used to recover the secret isogeny in polynomial time.

Our attack differs from the GPST adaptive attack as follows. In the GPST adaptive attack, the malicious Bob computes isogenies of correct degrees N_B and manipulates torsion point images. Our attack consists of computing isogenies of degrees larger than N_B and scaling the torsion point images by a suitable scalar to make the public key pass the pairing-based key validation method in SIDH. One then utilises the torsion point attack to recover the secret.

We prove that our attack runs in polynomial time. We provide specific attack parameters for SIDH primes \$IDHp182, \$IDHp217, SIDHp377, SIDHp434, SIDHp503 and SIDHp546. For these SIDH primes, the attack fully recovers Bob's secret isogeny querying a few tens of thousand times the key exchange key exchange oracle. Determining specific attack parameters for BSIDH primes is computationally intensive. We only give an example of generic attack parameters for the smallest BSIDH prime. We suggest countermeasures among which the Fujisaki-Okamoto transform (as used in SIKE), using SIDH proof of isogeny knowledge as recently proposed in [14] or setting the starting curve in SIDH to be a random supersingular curve with unknown endomorphism ring.

The torsion point attacks do not apply to SIDH parameters [11, §1.1 Figure 1] since they do not (yet) outperform generic passive attacks such as the meet in the middle on SIDH parameters. This attack comes as an ice breaker. This result, despite being less efficient when compared to the GPST adaptive attack, it proves that the torsion point attacks become relevant to SIDH and BSIDH parameters in an adaptive attack setting. Moreover, this attack vector is the first of its kind. It exploits the fact that in an SIDH instance, the pairing check does not suffices to convince Alice that Bob effectively computed an isogeny of degree N_B. We believe this attack fosters the understanding of SIDH and is a new cryptanalytic tool for isogeny based cryptography.

Outline. The remaining of this paper is organized as follows: in Section 2, we recall some generalities about elliptic curves and isogenies. We briefly present SIDH and the GPST adaptive attack. In Section 3, we present the torsion point attacks and describe our generalisation. In Section 4 we present an overview of our attack and describe the active phase. We also discuss the computation of the attack parameters and summarize the attack. In Section 5, we suggest attack

parameters for some SIDH primes and we briefly describe some countermeasures. We conclude the paper in Section 6.

2 Preliminaries

2.1 Elliptic curves and isogenies

An elliptic curve is a rational smooth curve of genus one with a distinguished point at infinity. Elliptic curves can be seen as commutative groups with respect to a group addition having the point at infinity as neutral element. When an elliptic curve E is defined over a finite field $\mathbb{F}_q$, the set of $\mathbb{F}_q$-rational points $E(\mathbb{F}_q)$ of E is a subgroup of E. For every integer N coprime with q, the N-torsion subgroup $E[N]$ of E is isomorphic to $\mathbb{Z}_N \oplus \mathbb{Z}_N$.

An isogeny from E to E' is a rational map from E to E' which is also a group morphism. The kernel of an isogeny is always finite and entirely defines the isogeny up to powers of the Frobenius. Given a finite subgroup G of E, there exists a Frobenius free isogeny of domain E having kernel G, called a separable isogeny. Its degree is equal to the size of its kernel. The co-domain of this isogeny is denoted by E/G. The isogeny and the co-domain E/G can be computed from the knowledge of the kernel using Vélu's formulas [34] whose efficiency depends on the smoothness of the isogeny degree.

An endomorphism of an elliptic curve E is an isogeny from E to E. The structure of E is closely related to that of its endomorphism ring. When E is defined over a finite field, the endomorphism ring of E is either an order in a quadratic field, in which case we say E is ordinary, or a maximal order in a quaternion algebra in which case we say E is supersingular. The generic isogeny problem is harder to solve for supersingular curves (for which the best attacks are exponential) than ordinary curves (for which there exists a sub-exponential attack [3]). SIDH is based on supersingular isogenies.

We refer to the book of Washington [37] and the book of Silverman [33] for more background on elliptic curves and isogenies. For a quick introduction to isogeny-based cryptography, we recommend these notes [13] from De Feo.

2.2 SIDH: Supersingular Isogeny Diffie-Hellman

The SIDH scheme is defined as follows.

Setup. Let $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ be a prime such that $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$. Let E_0 be a supersingular curve defined over $\mathbb{F}_{p^2}$. Set $E_0[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$ and $E_0[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$. The public parameters are E_0, p, ℓ_A, ℓ_B, e_A, e_B, P_A, Q_A, P_B, Q_B.

KeyGeneration. The secret key sk_A of Alice is a uniformly random integer α sampled from $\mathbb{Z}_{\ell_A^{e_A}}$. Compute the cyclic isogeny $\phi_A : E_0 \to E_A = E_0/\langle P_A + [\alpha]Q_A\rangle$. The public key of Alice is the tuple $\mathsf{pk}_A = (E_A, \phi_A(P_B), \phi_A(Q_B))$. Analogously, Bob's secret key sk_B is a uniformly random integer β sampled from $\mathbb{Z}_{\ell_B^{e_B}}$ and his public key is $\mathsf{pk}_B = (E_B, \phi_B(P_A), \phi_B(Q_A))$ where $\phi_B : E_0 \to E_B =$

$E_0/\langle P_B + [\beta]Q_B\rangle$.

KeyExchange. Upon receiving Bob's public key (E_B, R_a, S_a), Alice checks[5] that $e(R_a, S_a) = e(P_A, Q_A)^{\ell_B^{e_B}}$, 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 $e(R_b, S_b) = e(P_B, Q_B)^{\ell_A^{e_A}}$, 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 $j(E_{AB})$.

The correctness of the key exchange follows from the fact that

$$E_A/\langle \phi_A(P_B) + [\beta]\phi_A(Q_B)\rangle \simeq E_0/\langle P_A + [\alpha]Q_A, P_B + [\beta]Q_B\rangle \simeq E_B/\langle \phi_B(P_A) + [\alpha]\phi_B(Q_A)\rangle\,.$$

The scheme is summarized in Figure 1.

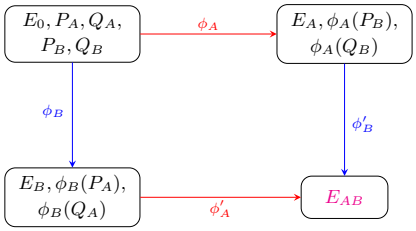

Fig. 1: SIDH Key Exchange

The security of the SIDH key exchange protocol against shared key recovery relies on Problem 1. Furthermore, Problem 2 states that it is difficult to distinguish the shared secret from a random supersingular elliptic curve.

Problem 1 (Supersingular Isogeny Computational Diffie-Hellman). Given E_0, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$, E_B, $\phi_B(P_A)$, $\phi_B(Q_A)$ (defined as in SIDH), compute E_{AB}.

Problem 2 (Supersingular Isogeny Decisional Diffie-Hellman). Given E_0, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$, E_B, $\phi_B(P_A)$, $\phi_B(Q_A)$ (defined as in SIDH) and a random supersingular curve E, distinguish between $E = E_{AB}$ and $E \neq E_{AB}$.

In the rest of this paper, we denote by N_A and N_B the degree of Alice's and Bob's isogeny respectively.

2.3 GPST adaptive attack

In SIDH [15] one does a pairing-based check on the torsion points $\phi_B(P_A)$ and $\phi_B(Q_A)$ returned by a potentially malicious Bob. Let E be a supersingular elliptic curve, let N be an integer and let μ_N be the group of N-roots of unity.

[5] Note that in the original SIDH [24], this pairing check is not part of the scheme. But, as precised in [9] and [20], one includes the check to discard some malformed public keys.

Let $e_N : E[N] \times E[N] \to \mu_N$ be the Weil pairing [19]. Let $\phi : E \to E'$ be an isogeny of degree M, then for $P, Q \in E[N]$,

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^M$$

where the first pairing is computed on E' and the second one on E.
In SIDH, given (E_B, R_a, S_a) returned by Bob as public key, Alice checks if

$$e_{\ell_A^{e_A}}(R_a, S_a) = e_{\ell_A^{e_A}}(P_A, Q_A)^{\ell_B^{e_B}}.$$

As we will see below, this verification does not assure that the points R, S were honestly generated. More precisely, the pairing verification does not capture the GPST adaptive attack.

The GPST adaptive attack. The main idea of the Galbraith et al. adaptive attack [20] is that if Bob manipulates the torsion points $\phi_B(P_A)$ and $\phi_B(Q_A)$ conveniently, then he can get some information about Alice's private key α given that he knows if the secret curve computed by Alice is equal to E_{AB} or not. Hence in the attack scenario, Bob needs to have access to the later information. This access is provided to Bob through a key exchange oracle:

$$O(E, R, S, E') \text{ which returns 1 if } j(E') = j(E/\langle R + [\alpha]S\rangle) \text{ and 0 otherwise}$$

If one supposes that $\ell_A = 2$ and $e_A = n$, then after each query, Bob recovers one bit of

$$\alpha = \alpha_0 + 2^1\alpha_1 + 2^2\alpha_2 + \cdots + 2^{n-1}\alpha_{n-1}.$$

Concretely, let us suppose that Bob has successfully recovered the first i bits of α, say $K_i = \alpha_0 + 2^1\alpha_1 + \cdots + 2^{i-1}\alpha_{i-1}$ so that

$$\alpha = K_i + 2^i\alpha_i + 2^{i+1}\alpha'$$

He generates $(E_B, \phi_B(P_A), \phi_B(Q_A))$ and computes the resulting key E_{AB}. To recover α_i, he chooses suitable integers a, b, c, d and queries the oracle O on (E_B, R, S, E_{AB}) where $R = [a]\phi_B(P_A) + [b]\phi_B(Q_A)$ and $S = [c]\phi_B(P_A) + [d]\phi_B(Q_A)$. The integers a, b, c and d are chosen to satisfy the following conditions:

1. if $\alpha_i = 1$, $\langle R + [\alpha]S\rangle = \langle \phi_B(P_A) + [\alpha]\phi_B(Q_A)\rangle$;
2. if $\alpha_i = 0$, $\langle R + [\alpha]S\rangle \neq \langle \phi_B(P_A) + [\alpha]\phi_B(Q_A)\rangle$;
3. the Weil paring $e_{2^n}(R, S)$ must be equal to $e_{2^n}(\phi_B(P_A), \phi_B(Q_A))$

The first two conditions help to distinguish the bit α_i. The third one prevents the attack from being detected by the pairing-based check presented in Section 2.3. When attacking the ith bit of alpha where $1 \leq i \leq n-2$, the attack uses the integers

$$a = \theta, \quad b = -\theta 2^{n-i-1}K_i, \quad c = 0, \quad d = \theta(1 + K_i 2^{n-i-1})$$

where $\theta = \sqrt{(1 + 2^{n-i-1})^{-1}}$. The attack recovers the first $n-2$ bits of α using $n-2$ oracle queries, and it recovers the two remaining bits by brute force. We refer to [20] for more details.

The GPST adaptive attack exploits the fact that the pairing check does not convince Alice that the torsion points returned by Bob were honestly computed. In the rest of this paper, we will design a new adaptive attack that exploits the fact that the pairing check does not convince Alice that Bob effectively computed an isogeny of degree N_B.

3 Generalizing torsion points attacks

In this section, we revisit the torsion point attacks. Firstly, we describe the torsion point attacks. Next, we provide a generalisation of these attacks that can be used to solve weaker version of the key recovery problem in SIDH (Problem 3, described below).

3.1 Torsion points attacks on SIDH

The direct key recovery attack (attacking one party's secret key) in SIDH translates into solving the following *Computational Supersingular Isogeny Problem.*

Problem 3. Let N_A and N_B be two smooth[6] integers such that $\gcd(N_A, N_B) = 1$. Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Set $E_0[N_B] = \langle P, Q \rangle$ and let $\phi : E_0 \to E$ be a random isogeny of degree N_A. Given E_0, E, P, Q, $\phi(P)$ and $\phi(Q)$, compute ϕ.

The difference between Problem 3 and the general isogeny problem is the fact that the action of ϕ on the group $E_0[N_B]$ is revealed. In 2017, Petit [29] exploited these torsion point images and the knowledge of the endomorphism ring of the starting curve E_0 to design an algorithm that solves Problem 3 for a certain choice of unbalanced ($N_A \ll N_B$) parameters. Petit's attack has recently been considerably improved by de Quehen et al. [11].

The idea of the torsion points attacks is to find a trace 0 endomorphism $\theta \in \mathrm{End}(E_0)$ that can be efficiently evaluated on $E_0[N_B]$, an integer d and a small smooth integer e such that

$$N_A^2 \deg \theta + d^2 = N_B^2 e. \tag{1}$$

Writing Equation 1 in terms of isogenies we get

$$\phi \circ \theta \circ \widehat{\phi} + [d] = \psi_2 \circ \psi_e \circ \psi_1 \tag{2}$$

where ψ_1 and ψ_2 are isogenies of degree N_B, ψ_e is an isogeny of degree e. The torsion point information $\phi(P)$, $\phi(Q)$ is used to evaluate $\tau = \phi \circ \theta \circ \widehat{\phi} + [d]$ on

[6] In all this paper, an integer is said to be smooth if it is b-smooth for some integer $b \approx O(\log p)$ where p is the characteristic of the base field considered.

$E[N_B]$. Knowing τ on $E_0[N_B]$, the kernels of the isogenies $\psi_1 : E \to E_1$ and $\widehat{\psi_2} : E \to E_2$ can be recovered efficiently. The isogeny $\psi_e : E_1 \to E_2$ is recovered by brute force or meet in the middle. We refer to [11, § 4.1] for technical details.

Having computed $\psi_2 \circ \psi_e \circ \psi_1$, one recovers

$$\ker \widehat{\phi} = \ker \left(\psi_2 \circ \psi_e \circ \psi_1 - [d]\right) \cap E[N_A].$$

Figure 2 illustrates the attack.

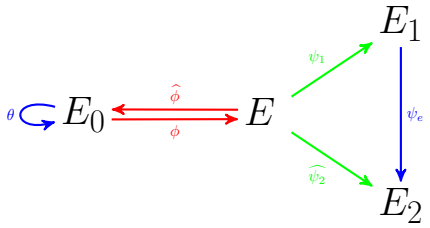

Fig. 2: Improved torsion points attack.

The efficiency of torsion point attacks mostly depends on the imbalance between the isogeny degree N_A and the order N_B of the torsion points images.

de Quehen et al. [11] show that under some heuristics, when $j(E_0) = 1728$, Problem 3 can be solved in:

1. Polynomial time when: $N_B > pN_A$ and $p > N_A$;
2. Superpolynomial time but asymptotically more efficient than meet-in-the-middle on a classical computer when: $N_B > \sqrt{p}N_A$;
3. Superpolynomial time but asymptotically more efficient than quantum claw-finding [25] when: $N_B > \max\{N_A, \sqrt{p}\}$.

More concretely, if $N_A \approx p^\alpha$ and $N_B \approx N_A p^\eta$, then the improved torsion points attack runs in time $\tilde{O}\left(N_A^{\frac{1+2(\alpha-\eta)}{4\alpha}}\right)$ and $\tilde{O}\left(N_A^{\frac{1+2(\alpha-\eta)}{8\alpha}}\right)$ on a classical computer and a quantum computer respectively [11, §6.2 Proposition 27]. In the special case where $\alpha = \frac{1}{2}$, we get the following corollary.

Corollary 1. *Suppose that $N_A \approx p^{\frac{1}{2}}$ and $N_B \approx p^{\frac{1}{2}+\eta}$ where $1 \leq \eta$. Under some heuristics, [11, Algorithm 7] solves Problem 3 in polynomial time when $j(E_0) = 1728$.*

Remark 1. SIKE parameters (for which E_0 is close to a curve having j-invariant 1728 and $N_A \approx N_B \approx \sqrt{p}$) are not affected by these improved torsion points attacks. Also, the attack does not affect any SIDH-type scheme in which the starting curve E_0 is a random supersingular curve with unknown endomorphism ring.

In our attack setting, we will not be provided with the images of torsion points through isogenies, but with the images of cyclic torsion groups. In the next section, we generalize the torsion point attacks such that they directly apply to our setting.

3.2 Generalized torsion points attacks

We consider the following problem.

Problem 4. Let N_A and N_B be two integers such that $\gcd(N_A, N_B) = 1$. Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let G_1, G_2, G_3 be three cyclic groups of E_0 of order N_B such that $G_1 \cap G_2 = G_1 \cap G_3 = G_2 \cap G_3 = \{0\}$. Let $\phi : E_0 \to E$ be a random isogeny of degree N_A.

Given E_0, G_1, G_2, G_3, E, $\phi(G_1)$, $\phi(G_2)$ and $\phi(G_3)$, compute ϕ.

The difference between Problem 4 and Problem 3 is the way the torsion point information is provided. In Problem 3, image points of a basis of the N_B-torsion group are given, while in Problem 4, only the images of three cyclic disjoint groups of order N_B are provided. This a priori represents less information, but as we show below, this is sufficient to run the improved torsion point attacks.

Let θ, d and e be such that Equation 1 is satisfied, set $\tau = \phi \circ \theta \circ \widehat{\phi} + [d]$. Let G_1, G_2 and G_3 be as in Problem 4. In the improved torsion point attacks, the torsion point information $(\phi(P), \phi(Q))$ is solely used to recover the action of τ on $E[N_B]$ as explained in Section 3.1. Hence we only need to prove that the knowledge of $\phi(G_1)$, $\phi(G_2)$ and $\phi(G_3)$ is sufficient to evaluate τ on $E[N_B]$.

First we prove that from the action of ϕ on 3 cyclic disjoint groups of order N_B, we can recover the image of a basis of $E_0[N_B]$ through $[\lambda] \circ \phi$ for some integer λ coprime to N_B. Concretely, we have the following lemma.

Lemma 1. *Let $\phi : E_0 \to E$ an isogeny of degree N_A and let N_B be a smooth integer coprime to N_A. Let $G_1 = \langle P_1 \rangle$, $G_2 = \langle P_2 \rangle$, $G_3 = \langle P_3 \rangle$ be three cyclic groups of E_0 of order N_B such that $G_1 \cap G_2 = G_1 \cap G_3 = G_2 \cap G_3 = \{0\}$. Given $H_1 = \langle Q_1 \rangle$, $H_2 = \langle Q_2 \rangle$, $H_3 = \langle Q_3 \rangle$ such that $\phi(G_i) = H_i$ for $i = 1, 2, 3$; there exists an integer $\lambda \in (\mathbb{Z}/N_B\mathbb{Z})^\times$ such that we can compute λ^2 and $[\lambda] \circ \phi(P)$ for any $P \in E_0[N_B]$.*

The result in Lemma 1 partially available in [2, Lemma 1 §3.2] where Basso et. al prove that from the action of ϕ on 3 well chosen cyclic groups of smooth order N_B, one can recover the action of ϕ on any group of order N_B. Our Lemma goes a bit further and proves that we can evaluate $[\lambda] \circ \phi$ on the N_B torsion for some $\lambda \in (\mathbb{Z}/N_B\mathbb{Z})^\times$ such that λ^2 is known. Note that knowing λ^2 does not always enable us to compute λ, since when N_B is not a prime power, the equation $x^2 \equiv a^2 \mod N_B$ may have more than two solutions.

Proof (of Lemma 1). For $i = 1, 2, 3$, set $\phi(P_i) = [\lambda_i]Q_i$ where $\lambda_i \in (\mathbb{Z}/N_B\mathbb{Z})^\times$. Since $G_1 \cap G_2 = \{0\}$, then $\{P_1, P_2\}$ is a basis of $E_0[N_B]$ and $\{Q_1, Q_2\}$ is a basis of $E[N_B]$. Write $P_3 = [v_1]P_1 + [v_2]P_2$ and $Q_3 = [u_1]Q_1 + [u_2]Q_2$. Then, we get

$$[\lambda_3 u_1]Q_1 + [\lambda_3 u_2]Q_2 = [\lambda_3]Q_3 = \phi(P_3) = [v_1]\phi(P_1) + [v_2]\phi(P_2) = [v_1\lambda_1]Q_1 + [v_2\lambda_2]Q_2.$$

Hence $\lambda_3 u_1 = v_1\lambda_1$, $\lambda_3 u_2 = v_2\lambda_2$ and $\lambda_i/\lambda_3 = u_i/v_i$ for $i = 1, 2$. Since $G_1 \cap G_3 = G_2 \cap G_3 = \{0\}$ and N_A is coprime to N_B, then $H_1 \cap H_3 = H_2 \cap H_3 = \{0\}$ and

$u_1, u_2, v_1, v_2 \in (\mathbb{Z}/N_B\mathbb{Z})^\times$. Thus $\lambda_1 v_1/u_1 = \lambda_3 = \lambda_2 v_2/u_2$, and $\phi(P_1) = [\lambda_3]Q_1'$, $\phi(P_2) = [\lambda_3]Q_2'$ where $Q_1' = [v_1/u_1]Q_1$ and $Q_2' = [v_2/u_2]Q_2$.

We have

$$e_{N_B}(P_1, P_2)^{\deg\phi} = e_{N_B}(\phi(P_1), \phi(P_2)) = e_{N_B}([\lambda_3]Q_1', [\lambda_3]Q_2') = e_N(Q_1', Q_2')^{\lambda_3^2}.$$

We recover λ_3^2 by solving the following discrete logarithm

$$\lambda_3^2 = DLP\left(e_{N_B}(P_1, P_2)^{\deg\phi}, e_{N_B}(Q_1', Q_2')\right).$$

For any $S = [\alpha]P_1 + [\beta]P_2 \in E_0[N_B]$ we have $[\lambda_3] \circ \phi(S) = [\alpha]Q_1' + [\beta]Q_2'$. □

Now that we can evaluate $[\lambda]\circ\phi$ point wise on $E_0[N_B]$ for some $\lambda \in (\mathbb{Z}/N_B\mathbb{Z})^\times$ such that λ^2 is provided, we show how to evaluate τ on $E[N_B]$.

Since we can evaluate $\phi_\lambda = [\lambda] \circ \phi$ on $E_0[N_B]$, then we can evaluate $\widehat{\phi_\lambda}$ on $E[N_B]$ as well. Therefore we can evaluate $\phi_\lambda \circ \theta \circ \widehat{\phi_\lambda}$ on $E[N_B]$. Meanwhile, we have

$$\phi_\lambda \circ \theta \circ \widehat{\phi_\lambda} = ([\lambda] \circ \phi) \circ \theta \circ ([\lambda] \circ \widehat{\phi}) = [\lambda^2] \circ \phi \circ \theta \circ \widehat{\phi}.$$

Since $\lambda^2 \in (\mathbb{Z}/N_B\mathbb{Z})^\times$ is provided, then we get

$$\phi \circ \theta \circ \widehat{\phi} = [\lambda^{-2}] \circ \phi_\lambda \circ \theta \circ \widehat{\phi_\lambda}$$

on $E[N_B]$. Hence $\tau = \phi \circ \theta \circ \widehat{\phi} + [d]$ can be efficiently evaluated on $E[N_B]$. This concludes our discussion.

From now on, we can translate the solutions in [11] computing θ, d, e, and using the torsion point attacks to solve Problem 3 into solutions that compute θ, d, e, and solve Problem 4 in the same time and memory complexity, ignoring polylogarithmic factors.

Theorem 1 (Generalized Torsion Point Attacks). *Suppose we are given an instance of Problem 4 where N_A has $O(\log\log p)$ distinct prime factors. Assume we are given the restriction of a trace-zero endomorphism $\theta \in End(E_0)$ to $E_0[N_B]$, an integer d coprime to N_B, and a smooth integer e such that*

$$\deg\left(\phi \circ \theta \circ \widehat{\phi} + [d]\right) = N_B^2 e \quad \text{or} \quad \deg\left(\phi \circ \theta \circ \widehat{\phi} + [d]\right) = N_B^2 pe.$$

Then we can compute ϕ in time $\tilde{O}(\sqrt{e})$.

Proof. Follows from the previous discussion, [11, Theorem 3] and [11, Theorem 5].

We have the following Corollary.

Corollary 2. *Suppose that $N_A \approx p^{\frac{1}{2}}$ and $N_B \approx p^{\frac{1}{2}+\eta}$ where $1 \leq \eta$. Under some heuristics, Problem 4 can be solved in polynomial time when $j(E_0) = 1728$.*

In the following section, we use the generalized torsion point attacks to design a new adaptive attack on SIDH.

4 A new adaptive attack on SIDH

In this section, we present our attack. First we present an overview, next we describe the active phase of our attack.

4.1 Overview

In our attack, we suppose that one party is using a static secret/public key pair, and the other party runs multiple key exchanges with the honest party. He is provided with a the same oracle $O(E, R, S, E')$ described in Section 2.3.

The main idea of the attack is to use a key exchange oracle to recover the action of Alice's secret isogeny on a larger torsion point group. Doing so leads to an unbalanced SIDH. The malicious Bob then uses the revisited torsion point attacks, which in this case run in polynomial time, to recover Alice's secret key. Hence our attack has two phases.

Let N_A and N_B be the isogeny degrees of Alice and Bob respectively. In general, we have $N_A N_B | p+1$ in the case of SIDH schemes, $N_A | p+1$, $N_B | p-1$ or $N_B | p+1$, $N_A | p-1$ for BSIDH. Let $E_0 = E(1728)$ be the starting curve, $E_0[N_B] = \langle P_B, Q_B \rangle$, and let $(E_A, \phi_A(P_B), \phi_A(Q_B))$ be Alice's public key where her static secret key is an isogeny $\phi_A : E_0 \to E_A$ of degree N_A. Moreover, suppose that you are given some "suitable" smooth integer N coprime to N_A such that $E_0[N_B N] \subset E_0(\mathbb{F}_{p^{2k}})$ for some integer k (we will provide the requirements on N as we describe the attack in the following sections).

The two phases of the attack can be summarized as follows.

- **The active phase.** Bob uses the access to a key exchange oracle $O(E, R, S, E')$ to secretly transform Alice's static public key $(E_A, \phi_A(P_B), \phi_A(Q_B))$ into a tuple $(E_A, \phi_A(G_1), \phi_A(G_2), \phi_A(G_3))$ where $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$, $G_3 = \langle R \rangle$ are cyclic subgroups of maximal order in $E_0[N_B N]$, such that $G_1 \cap G_2 = G_1 \cap G_3 = G_2 \cap G_3 = \{0\}$.
- **The passive phase.** Having $(E_A, \phi_A(G_1), \phi_A(G_2), \phi_A(G_3))$, Bob applies the revisited torsion point attacks to recover Alice's secret.

The passive phase is nothing else than the revisited torsion point attacks described in Section 3.2. In the rest of this section, we provide a full description of the active phase.

4.2 Explicit description of the active phase

Let p be the base prime. Let $N = \ell_1^{v_1} \cdots \ell_n^{v_n}$ be a smooth integer coprime to N_A such that $E_0[\ell_i^{v_i}] \subset E(\mathbb{F}_{p^{2k_i}})$ and for each prime ℓ_i which is not a square modulo N_A, v_i is even. Let G_1, G_2, G_3 be cyclic subgroups of $E_0[N_B N]$ or order $N_B N$ such that $G_1 \cap G_2 = G_1 \cap G_3 = G_2 \cap G_3 = \{0\}$. The active phase of the attack consists in recovering $\phi_A(G_j)$ for $j = 1, 2, 3$.

For $j = 1, 2, 3$, we can represent G_j as $G_j = \sum_{i=1}^{r} G_{ji}$ where G_{ji} is a group of order $N_B \ell_i^{v_i}$. The action of ϕ_A on G_j is recovered by computing $\phi_A(G_{ji})$ for $i =$

$1, \cdots, n$. Storing $\phi_A(G_j)$ in this form enables us to perform all computations in extension fields of degree $k_1, \cdots, k_n$, instead of $LCM(k_1, \cdots, k_n)$ the full group G_j is considered. This is because all supersingular isogenies are $\mathbb{F}_{p^2}$-rational. Hence we never go to extension fields with degree beyond $\max\{k_i, i = 1, \cdots, r\}$. Let us describe how we compute $\phi_A(G_{ji})$ for $j = 1, 2, 3$ and $i = 1, \cdots, n$.

Let G be a cyclic subgroup of $E_0[N_B\ell^v]$ of order $N_B\ell^v$. Let us suppose that $\ell \equiv \mu^2 \mod N_A$ is a square modulo N_A and that $v = 1$. Note that $\phi_A([\ell]G)$ is readily provided in Alice's public key since this group has order N_B. To compute the action of ϕ_A on G of order $N_B\ell$, Bob computes the isogeny $\phi_G : E_0 \to E_G$ having kernel G together with $R = [\mu^{-1}]\phi_G(P_A)$, $S = [\mu^{-1}]\phi_G(Q_A)$. Let H be a random cyclic subgroup of $E_A[N_B\ell]$ of order $N_B\ell$ containing $\phi_A([\ell]G)$. Let $\phi_H : E_A \to E_H$ be the isogeny of kernel H and $\phi'_A : E_G \to E_G/\phi_G(\ker(\phi_A))$ be the isogeny of kernel $\phi_G(\ker(\phi_A))$. Then if H is the image of the group G through ϕ_A then the diagram in Figure 3 commutes and $O(E_G, R, S, E_H) = 1$. In the other case, when $H \neq \phi_A(G)$, Lemma 2 shows that the oracle returns 1 with negligible probability.

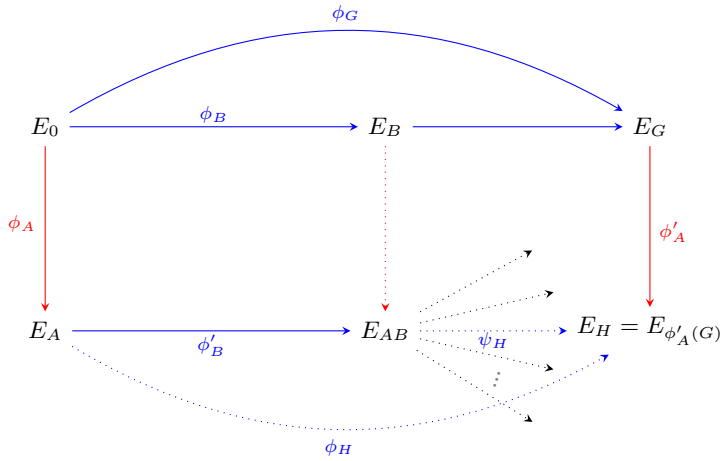

Fig. 3: Computing the action of ϕ_A on G.

Lemma 2. *Suppose that $\ell \approx O(\log p)$ and $N_AN_B \approx p$ (or $N_AN_B > p$), and let G, H, E_H and $E_G/\phi_G(\ker(\phi_A))$ be defined as above. If $H \neq \phi_A(G)$ then $E_H = E_G/\phi_G(\ker(\phi_A))$ with negligible probability.*

Proof. Suppose that $E_H = E_G/\phi_G(\ker(phi_A))$ and let $H' = \phi_A(G)$. Let $H' = \phi_A(G)$. By construction, we get $[\ell]H = [\ell]\phi_A(G) = [\ell]H'$, and we can decompose ϕ_H and ϕ'_H as $\phi_H = \psi_H \circ \phi'_B$ and $\phi_{H'} = \psi_{H'} \circ \phi'_B$ where ϕ_H and $\phi_{H'}$ are isogenies of degree ℓ from E_{AB} to $E_G/\phi_G(\ker(\phi_A))$. Since $H \neq H'$, then $\widehat{\psi_{H'}} \neq \pm\psi_H$ and $\widehat{\psi_{H'}} \circ \psi_H$ is a non scalar endomorphism of E_{AB} of degree ℓ^2. Therefore, the curve E_{AB} is an ℓ^2-small curve as defined in [28].

On the other hand, since $N_A N_B \approx p$, then E_{AB} is statistically a random supersingular curve [21]. Moreover, the number of ℓ^2-small curves is roughly ℓ^3 [28]. Considering the fact that the number of supersingular curves defined over $\mathbb{F}_{p^2}$ is $\frac{p}{12}$, then the probability that E_{AB} is an ℓ^2-small curve is at roughly $\frac{12\ell^3}{p}$, which is negligible since $\ell \approx O(\log p)$. □

Remark 2. We scale $\phi_G(P_A)$ and $\phi_G(Q_A)$ by μ^{-1} in order to avoid the detection by pairing computation. When scaled by μ^{-1}, we have

$$\begin{aligned} e_{N_A}(R,S) &= e_{N_A}([\mu^{-1}]\phi_G(P_A), [\mu^{-1}]\phi_G(Q_A)) \\ &= e_{N_A}(P_A, Q_A)^{\mu^{-2}\deg\phi_G} \\ &= e_{N_A}(P_A, Q_A)^{N_B}. \end{aligned}$$

The above equation also justifies the requirement that ℓ should be a quadratic residue modulo N_A. When ℓ is not a quadratic residue modulo N_A and ℓ^2 divides N, we set the group G to have order $N_B\ell^2$ and we proceed the same way. In the later case, we scale the points $\phi_G(P_A)$ and $\phi_G(Q_A)$ by $\ell^{-1} \mod N_A$ instead.

If $1 < v$, then the process can be iterated to recover the action of ϕ_A on groups of order $N_B\ell, N_B\ell^2, \cdots, N_B\ell^v$ when ℓ is a square modulo N_A, respectively $N_B\ell^2$, $N_B\ell^4, \cdots, N_B\ell^v$ when ℓ is not a quadratic residue modulo N_A. Note that in the later case, v is even.

We deduce Algorithm 1 for computing the action of ϕ_A on a larger group G.

Lemma 3. *Algorithm 1 runs in time $\tilde{O}(k_v) = O(k_v \cdot \mathrm{poly}(\log p))$ time whenever ℓ is of polynomial size and $E_0[N_B\ell^v] \subset E(\mathbb{F}_{p^{2k_v}})$. The output of Algorithm 1 is $\phi_A(G)$ with overwhelming probability.*

Proof. Since ℓ, N_A and N_B are smooth integers, the time complexity of Algorithm 1 depends on the degree k_v of the field extension only. Hence Algorithm 1 runs in time $O(k_v \cdot \mathrm{poly}(\log p))$. The second point of the Lemma follows from Lemma 2. □

Recall that $E_0[N_B\ell_i^{v_i}] \subset E(\mathbb{F}_{p^{2k_i}})$. Set $k^* = \max\{k_i\}$. Algorithm 2 fully describes the active phase our attack.

Lemma 4. *Algorithm 2 runs in time $\tilde{O}(\max\{k^*\})$ whenever ℓ_i for $i = 1, \cdots, n$, N_A, N_B are smooth integers.*

Proof. Follows from the Lemma 3. □

This concludes our description of the active phase. In the next section, we discuss the computation of the integer N.

Algorithm 1 Evaluating the action of ϕ_A on a larger group G of order $N_B\ell^v$ using $O(E, R, S, E')$.

Require: E_0, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$, G.
Ensure: $\phi_A(G)$.
Set $G_0 = [\ell^v]G$;
if ℓ is a square modulo N_A **then**
  Compute $\mu = \sqrt{\ell} \mod N_A$;
  for $i = 1, \cdots, v$ **do**
    $G_i = [\ell^{v-i}]G$
    Compute $\phi_{G_i} : E_0 \to E_{G_i}$ of degree $N_B\ell^i$ and of kernel G_i, together with $R = [\mu^{-i}]\phi_{G_i}(P_A)$ and $S = [\mu^{-i}]\phi_{G_i}(Q_A)$;
    for H cyclic group of E_A of order $N_B\ell^i$ containing $\phi_A(G_{i-1})$ **do**
      Compute $\phi_H : E_A \to E_H$ of kernel H;
      if $O(E_{G_i}, R, S, E_H) = 1$ **then**
        Set $\phi_A(G_i) = H$;
  $G' = \phi_A(G_v)$;
else
  for $i = 1, \cdots, v/2$ **do**
    $G_i = [\ell^{v-2i}]G$
    Compute $\phi_{G_i} : E_0 \to E_{G_i}$ of degree $N_B\ell^{2i}$ and of kernel G_i, together with $R = [\ell^{-i}]\phi_{G_i}(P_A)$ and $S = [\ell^{-i}]\phi_{G_i}(Q_A)$;
    for H cyclic group of E_A of order $N_B\ell^{2i}$ containing $\phi_A(G_{i-1})$ **do**
      Compute $\phi_H : E_A \to E_H$ of kernel H;
      if $O(E_{G_i}, R, S, E_H) = 1$ **then**
        Set $\phi_A(G_i) = H$;
  $G' = \phi_A(G_{v/2})$;
return G'.

Algorithm 2 Recovering the action of ϕ_A on cyclic disjoint groups G_1, G_2, G_3 of order N_BN using the oracle $O(E, R, S, E')$

Require: E_0, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$, N_A, N_B, $N = \ell_1^{v_1} \cdots \ell_n^{v_n}$, G_{ji} for $j = 1, 2, 3$ and $i = 1, \cdots, n$.
Ensure: $\phi_A(G_{ji})$ for $j = 1, 2, 3$ and $i = 1, \cdots, r$.
for $i = 1, \cdots, n$ **do**
  for $j = 1, 2, 3$ **do**
    Compute $\phi_A(G_{ji})$ using Algorithm 1;
return $\phi_A(G_{ji})$ for $j = 1, 2, 3$ and $i = 1, \cdots, n$.

4.3 Computing the integer N

We address the existence and the computation of the integer N. We would like to compute a smooth integer $N = \ell_1^{v_1} \cdots \ell_n^{v_n}$ coprime to N_A such that $E_0[N_B\ell_i^{v_i}] \subset E(\mathbb{F}_{p^{2k_i}})$ and for each prime ℓ_i which is not a square modulo N_A,

v_i is even. Recall that by Corollary 2, the torsion point attacks run in polynomial time when $p < N$.

We start by the following Lemma which describes the group structure of supersingular curves over extension fields.

Lemma 5. *Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve such that $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}_{p-\epsilon})^2$ where $\epsilon = \pm 1$ corresponds to the sign of the trace of Frobenius $t = 2\epsilon p$ of E over $\mathbb{F}_{p^2}$.*
Then for every natural number k, the group structure of E over $\mathbb{F}_{p^{2k}}$ is given by

$$E(\mathbb{F}_{p^{2k}}) \simeq (\mathbb{Z}_{p^k-\epsilon^k})^2 \tag{3}$$

Proof. Let k be natural number and let t_k be the trace of Frobenius of E over $\mathbb{F}_{p^{2k}}$. Then by Hasse Theorem (theorem V.1.1 of [34]),

$$|E(\mathbb{F}_{p^{2k}})| = p^{2k} + 1 - t_k.$$

Over $\mathbb{F}_{p^2}$, the characteristic equation of Frobenius is given by

$$X^2 - 2\epsilon pX + p^2 = (X - \epsilon p)^2$$

By Theorem 4.12 of [37]

$$t_k = 2(\epsilon p)^k = 2\epsilon^k p^k$$

where ϵ^k is the sign of t_k. Hence $\quad t_k^2 = 4p^{2k} \quad$ and by lemma 4.8 of [32]

$$E(\mathbb{F}_{p^{2k}}) \simeq (\mathbb{Z}_{\sqrt{p^{2k}}-\epsilon^k})^2 \simeq (\mathbb{Z}_{p^k-\epsilon^k})^2.$$

□

From Equation 3, we have that $E_0[N_B\ell_i^{v_i}] \subset E_0(\mathbb{F}_{p^{2k_i}})$ if and only if $N_B\ell_i^{v_i} | p^{k_i} - \epsilon^{k_i}$ where ϵ is the sign of the trace of Frobenius of E_0 as described in the proof of Lemma 5.

Let ℓ be a small prime. Then $\ell^v | p^{2k} - 1$ for some $k \leq \ell^v$. This means that for each prime ℓ_i dividing N, $k_i \leq \ell_i^{v_i}$. This heals a easy way to compute N : choose the smallest primes ℓ_i coprime to $N_A N_B$, such that $p < N = \prod \ell_i^2$. Then the largest ℓ_i is in $O(\log p)$. Moreover we have k_i at most ℓ_i^2.

To moderate the fields extension degrees, we also include in N primes ℓ that are squares modulo N_A. For this primes, we only require ℓ to divide $p^{2k} - 1$, hence obtaining a smaller field extension.

We describe the full process in Algorithm 3. The algorithm returns the list P of prime power factors of N with the list D of the corresponding extension field degrees.

Lemma 6. *Algorithm 3 runs in polynomial time and for each prime ℓ_i dividing N, $k_i \leq \ell_i^2 \approx O(\log^2 p)$.*

Proof. Follows from the previous discussion. □

Algorithm 3 Computing N

Require: p, N_A, N_B.
Ensure: P, D.
1: Create the lists P and D, set $N = 1$, set $\ell = 1$;
2: **while** $N < p$ **do**
3: choose the next prime ℓ coprime to $N_A N_B$;
4: **if** ℓ is a square modulo N_A **then**
5: Compute the smallest integer k such that $\ell | p^{2k} - 1$.
6: Append ℓ to the list P and $2k$ to the list D;
7: $N = N * \ell$;
8: **else**
9: Compute the smallest integer k such that $\ell^2 | p^{2k} - 1$.
10: Append ℓ^2 to the list P and $2k$ to the list D;
11: $N = N * \ell^2$;
12: **return** P, D;

Remark 3. In all this section, we were attacking Alice's secret isogeny. To attack Bob's secret isogeny instead, one interchanges the roles of N_A and N_B. Mostly, the quadratic residuosity condition on N will depend on N_B.

Remark 4. In practice, on may set a bound a bound on the extension degrees and slightly increase the size of the primes ℓ_i. This will be the case in the attack parameters we will present in Section 5.

4.4 Attack summary

The full attack can is summarised in Algorithm 4.

Algorithm 4 New Adaptive attack on SIDH

Require: E_0, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$, N_A, N_B.
Ensure: $\ker(\phi_A)$.
1: Compute a suitable smooth integer N using Algorithm 3.
2: Let G_1, G_2, G_3 cyclic disjoint subgroups of $E_0[N_B N]$ of order $N_B N$.
3: Compute $\phi_A(G_1)$, $\phi_A(G_2)$, $\phi_A(G_3)$ using the oracle $O(E, R, S, E')$ and Algorithm 2.
4: Compute ϕ_A using the revisited torsion point attacks of Theorem 1.
5: **return** $\ker(\phi_A)$.

Now we evaluate the number of oracle queries. Since $N = \ell_1^{v_1} \cdots \ell_n^{v_n}$ where for each prime ℓ_i which is not a square modulo N_A, v_i is even, then we can write $N = \ell_1^{2v_1} \cdots \ell_n^{2v_n} \ell_{n+1}^{u_1} \cdots \ell_{n+m}^{u_m}$ where the primes ℓ_{n+j} for $j = 1, \cdots, m$ are squares modulo N_A. From Algorithm 1, for each prime factor ℓ_i $(1 \leq i \leq n)$ of N, the maximum number of queries to the oracle (E, R, S, E') is equal to the number of cyclic subgroups of $\left(\mathbb{Z}/\ell_i^2\mathbb{Z}\right)^2$ order ℓ_i^2, which is $\ell_i(\ell_i + 1)$. Note that if

the first $\ell_i(\ell_i+1)-1$ queries fail, then there is no need to perform the last query since it will succeed. Also, for each prime factor ℓ_{n+j} $(1 \leq j \leq m)$ of N, the maximum number of queries to the oracle (E, R, S, E') is equal to the number of cyclic subgroups of $(\mathbb{Z}/\ell_i\mathbb{Z})^2$ order ℓ_i, which is $\ell_i + 1$. Here also, there is no need to perform the last query when the first ℓ_i queries failed. Therefore, the maximum number of oracle queries in the attack is

$$O_q = \sum_{i=1}^{n} v_i \left[\ell_i(\ell_i+1) - 1\right] + \sum_{j=1}^{m} u_j \ell_{n+j}.$$

Now we can state the main result of this paper.

Theorem 2. *Let p, E_0, $N_A < p$, $N_B < p$, P_A, Q_A, P_B, Q_B, E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$ be the public parameters and the public key of an SIDH type scheme.*

Provided a key exchange oracle $O(E, R, S, E')$, Algorithm 4 recovers ϕ_A in polynomial time.

Furthermore, Algorithm 4 performs at most

$$O_q = \sum_{i=1}^{n} v_i \left[\ell_i(\ell_i+1) - 1\right] + \sum_{j=1}^{m} u_j \ell_{n+j}$$

queries to the key exchange oracle where $N = \ell_1^{2v_1} \cdots \ell_n^{2v_n} \ell_{n+1}^{u_1} \cdots \ell_{n+m}^{u_m}$ is the integer computed in Step 1.

Proof. By Lemma 3, Step 1 outputs a smooth integer N such that $\max\{k_i\} \approx O(\log^2 p)$. Hence by Lemma 3, Step 3 runs in time $\tilde{O}(\log^2 p) = \tilde{O}(1)$. Step 4 runs in polynomial time since $p < N$. The number of oracle queries follows from the discussion preceding Theorem 2. □

Remark 5. In our attack, the malicious Bob computes isogenies of degree $N_B\ell^2$ or $N_B\ell$ depending on the quadratic residuosity of ℓ modulo N_A. In appendix A, we suggest a variant of the attack where isogenies Bob computes isogenies of degree ℓ^2 or ℓ instead. Nevertheless, this variant can be easily detected.

5 Relevance and countermeasures

In this section, we suggest some attack parameters for $IDH and SIDH primes. We discuss possible countermeasures to the attack.

5.1 Attack parameters for some SIDH primes

We propose attack parameters for the two (non cryptographic size) primes suggested for the $IKE challenge [8, §10], the SIDH primes SIDHp377 and SIDHp546 suggested by Longa et. al [27], SIDHp434 and SIDHp503 as specified in SIKE [23].

As attack parameters, we provide the prime factorisation of N, the maximum field extension degree $k^* = \max\{k_i\}$, $\eta \approx N/p$ and the number O_q of oracle queries. We also precise which party is attacked: B stands for Bob and A stands for Alice.

The outcome of our investigations on the above mentioned \$IDH primes and SIDH primes is summarised in Table 1 and Table 2 respectively.

Party	k^*	η	O_q	N
\$IDHp182 prime: $p = 2^{91}3^{57} - 1$				
B	96	$\frac{185}{182}$	7251	$5^2 * 7 * 11^2 * 13 * 19 * 31 * 37 * 43 * 47^2 * 61 * 67 * 73 * 79 * 97 * 103 * 109 * 127 * 139 * 157 * 181 * 241 * 277 * 421 * 433 * 541 * 661 * 919$
\$IDHp217 prime: $p = 2^{110}3^{67} - 1$				
B	96	$\frac{222}{217}$	9349	$5^2 * 7 * 13 * 19 * 31 * 37 * 43 * 61 * 67 * 73 * 79 * 97 * 109 * 157 * 163 * 181 * 193 * 199 * 211 * 223 * 229 * 271 * 277 * 307 * 337 * 571 * 631 * 1009 * 1093 * 1249 * 1381$

Table 1: Attack parameters for the two \$IDH primes.

When it comes to BSIDH instances, generating specific attack parameters is less trivial. We believe this may be because BSIDH primes[7] are twin primes. Using the generic attack parameters computation described in Algorithm 3, the degree of the field extensions are relatively larger compared to those used when running the attack on SIDH. For example, let us consider the smallest BSIDH prime (prime in example 6 of [7])

$$p = 2 \cdot (2^3 \cdot 3^4 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 53^2)^6 - 1.$$

Set $N_A = p + 1$ and $N_B = p - 1$. Then we get

$$N = 5^2 \cdot 11^2 \cdot 23^2 \cdot 29^2 \cdot 41^2 \cdot 47^2 \cdot 59^2 \cdot 61^2 \cdot 67^2 \cdot 71^2 \cdot 79^2 \cdot 83^2 \cdot 89^2 \cdot 97^2 \cdot 101^2 \cdot 107^2 \cdot 109^2 \cdot 113^2 \cdot 127^2 \cdot 131^2 \cdot 137^2$$

and the ℓ_i^2 torsion points for ℓ_i dividing N are defined over extension fields of $\mathbb{F}_{p^2}$ of degree

$$20, 55, 253, 406, 820, 23, 3422, 15, 402, 2485, 3081, 3403, 1958, 9312, 2020, 5671, 11772, 12656, 8001, 1310, 2329,$$

the order is the same as in the prime factorisation of N. The number of oracle queries is $O_q = 152523$. Note that here, one will be working with extension fields of degree up to 12656. One may prefer to compute a different integer N for which the maximum extension field degree is relatively small, but as we mentioned before, this requires intensive computations which we could not do on a personal computer.

[7] Primes p such that both $p + 1$ and $p - 1$ are smooth.

Party	k	η	O_q	N
SIDHp377 prime: $p = 2^{191}3^{117} - 1$				
B	120	$\frac{377}{377}$	40728	$5^2 * 7 * 11^2 * 13 * 19 * 31 * 37 * 43 * 61 * 67 * 73 * 79 * 97 * 103 * 109 * 157 * 181 * 193 * 199 * 229 * 241 * 271 * 277 * 307 * 313 * 331 * 337 * 433 * 487 * 571 * 631 * 661 * 739 * 1009 * 1021 * 1051 * 1093 * 1249 * 1993 * 2161 * 2707 * 3433 * 3529 * 4003 * 4603 * 5419$
SIDHp434 prime: $p = 2^{216}3^{137} - 1$				
B	152	$\frac{438}{434}$	66169	$5^2 * 7 * 11^2 * 13 * 17^2 * 19 * 31 * 37 * 43 * 61 * 67 * 71^2 * 73 * 79 * 97 * 103 * 109 * 127 * 139 * 151 * 181 * 193 * 211 * 277 * 373 * 409 * 421 * 433 * 457 * 547 * 601 * 613 * 739 * 751 * 757 * 1123 * 1171 * 1231 * 1489 * 1741 * 1873 * 2311 * 2593 * 2887 * 3037 * 3061 * 4357 * 5227 * 6091 * 6661 * 7621$
SIDHp503 prime: $p = 2^{250}3^{159} - 1$				
B	158	$\frac{512}{503}$	81049	$5^2 * 7 * 11^2 * 13 * 19 * 31 * 37 * 43 * 61 * 67 * 73 * 79 * 97 * 103 * 109 * 127 * 139 * 151 * 157 * 163 * 181 * 193 * 199 * 211 * 229 * 241 * 277 * 409 * 421 * 433 * 439 * 457 * 463 * 571 * 577 * 601 * 859 * 967 * 1093 * 1153 * 1171 * 1201 * 1303 * 1327 * 1741 * 2131 * 2179 * 2269 * 2371 * 2377 * 2689 * 3037 * 3169 * 4663 * 6151 * 6469 * 6529 * 8893 * 9769$
SIDHp546 prime: $p = 2^{273}3^{172} - 1$				
B	152	$\frac{551}{546}$	112441	$5^2 * 7 * 11^2 * 13 * 19 * 31 * 37 * 43 * 61 * 67 * 73 * 79 * 83^2 * 97 * 103 * 109 * 127 * 139 * 151 * 157 * 163 * 181 * 193 * 223 * 277 * 307 * 379 * 409 * 421 * 433 * 457 * 613 * 631 * 661 * 691 * 751 * 1117 * 1153 * 1249 * 1321 * 1621 * 1741 * 1753 * 1801 * 1933 * 1999 * 2053 * 2137 * 2281 * 3571 * 3823 * 5059 * 5281 * 5563 * 6373 * 6397 * 6481 * 7549 * 7639 * 8161 * 9151$

Table 2: Attack parameters for some SIDH primes.

Remark 6. Our attack applies to eSIDH [4] as well. It can be easily adapted to k-SIDH [1] and it's variant by Jao and Urbanik [35]. In the later case, the number of oracle queries is exponential in k.

5.2 Countermeasures to the attack

A straightforward countermeasure of the attack is to use a variant of the Fujisaki-Okamoto transform [18,22] as in SIKE. This transform obliges Bob to disclose his secret key to Alice who will recompute Bob's public to verify its correctness. Recomputing Bob's public key will enable Alice to detect Bob's maliciousness.

A second countermeasure is that Bob uses the SIDH proof of Knowledge as recently suggested in [14]. In this proof of knowledge, Bob proves that there exists an isogeny of degree N_B between E_0 and E_B and that the provided torsion points were not maliciously computed. Nevertheless, this countermeasure is very costly, since the proof of isogeny knowledge is nothing else than the SIDH based signature scheme, which is relatively slow and has large signatures.

Another less costly countermeasure is to set the curves E_0 to be a random supersingular elliptic curve with unknown endomorphism ring. This counters the improved torsion points attack. Hence Bob will not be able to recover Alice's secret isogeny after recovering its action on a larger torsion group. Nevertheless, one should keep in mind that this later countermeasure does not counter the GPST adaptive attack.

6 Conclusion

In this paper, we generalized the torsion point attacks in such a way that they can be used to recover a secret isogeny provided its action on three disjoint cyclic subgroup of relatively large order. We then used this generalized torsion point attacks to design a new adaptive attack on SIDH type schemes. The attack consists of maliciously computing isogenies of larger degrees than expected in SIDH, then using an access to the key exchange oracle to recover the action of the honest party's secret isogeny on a larger torsion groups. Afterwards, one obtains an unbalanced SIDH instance on which one applies the generalized torsion points attack to recover the honest party's secret isogeny. Our attack runs in polynomial time.

We provide concrete attack parameters for SIDH instances instantiated with the SIDH primes \$IDHp182, \$IDHp217, SIDHp377, SIDHp434, SIDHp546 and SIDHp503. A search of attack parameters on BSIDH primes is ongoing. We finally suggest countermeasures among which the Fujisaki-Okamoto transform (as used in SIKE), using a proof of isogeny knowledge as recently proposed in [14] or setting the starting curve in SIDH to be a random supersingular curve with unknown endomorphism ring.

This result proves that torsion point attacks, which do not yet apply to SIDH, become relevant to SIDH parameters in an adaptive attack setting. Moreover, it introduces a new cryptanalytic tool for isogeny based cryptography.

Acknowledgements. We would like to thank the anonymous reviewers for their valuable comments and feedback.

References

1. Reza Azarderakhsh, David Jao, and Christopher Leonardi. Post-quantum static-static key agreement using multiple protocol instances. In *International Conference on Selected Areas in Cryptography*, pages 45–63. Springer, 2017.
2. Andrea Basso, Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Antonio Sanso. Cryptanalysis of an oblivious PRF from supersingular isogenies. Cryptology ePrint Archive, Report 2021/706, 2021. https://ia.cr/2021/706.
3. Jean-Francois Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in Cryptology – INDOCRYPT 2014*, pages 428–442. Springer, 2014.
4. Daniel Cervantes-Vázquez, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez. eSIDH: the revenge of the SIDH. Cryptology ePrint Archive, Report 2020/021, 2020. https://ia.cr/2020/021.

5. Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.
6. Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.
7. Craig Costello. B-SIDH: Supersingular Isogeny Diffie-Hellman Using Twisted Torsion. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 440–463, Cham, 2020. Springer International Publishing.
8. Craig Costello. The Case for SIKE: A Decade of the Supersingular Isogeny Problem. Cryptology ePrint Archive, Report 2021/543, 2021. https://ia.cr/2021/543.
9. Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 572–601, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
10. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291.
11. Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Improved torsion point attacks on SIDH variants. Cryptology ePrint Archive, Report 2020/633, 2020. https://eprint.iacr.org/2020/633.
12. Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368. Springer, 2018.
13. Luca De Feo. Mathematics of isogeny based cryptography. *CoRR*, abs/1711.04062, 2017.
14. Luca De Feo, Samuel Dobson, Steven D. Galbraith, and Lukas Zobernig. SIDH Proof of Knowledge. Cryptology ePrint Archive, Report 2021/1023, 2021. https://ia.cr/2021/1023.
15. Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, 2014. Pagesn 209-247.
16. Tako Boris Fouotsa, Péter Kutas, and Simon-Philipp Merz. On the Isogeny Problem with Torsion Point Information. Cryptology ePrint Archive, Report 2021/153, 2021. https://eprint.iacr.org/2021/153.
17. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption. In Michael J. Wiener, editor, Advances in Cryptology-CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 537-554, Santa Barbara, CA, USA, August 15-19, 1999. Springer, Heidelberg, Germany.
18. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Annual International Cryptology Conference*, pages 537–554. Springer, 1999.
19. Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.
20. Steven D Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology – ASIACRYPT 2016*, pages 63–91. Springer, 2016.
21. Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 3–33. Springer International Publishing, 2017.

22. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.
23. 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.
24. 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.
25. Samuel Jaques and André Schrottenloher. Low-gate quantum golden collision finding. Cryptology ePrint Archive, Report 2020/424, 2020. https://eprint.iacr.org/2020/424.
26. P. Kutas, Simon-Philipp Merz, C. Petit, and Charlotte Weitkämper. One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols. *IACR Cryptol. ePrint Arch.*, 2021:282, 2021.
27. Patrick Longa, Wen Wang, and Jakub Szefer. The Cost to Break SIKE: A Comparative Hardware-Based Analysis with AES and SHA-3. Cryptology ePrint Archive, Report 2020/1457, 2020. https://ia.cr/2020/1457.
28. Jonathan Love and D. Boneh. Supersingular curves with small non-integer endomorphisms. *ArXiv*, abs/1910.03180, 2019.
29. 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.
30. Christophe Petit and Kristin E Lauter. Hard and easy problems for supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/962, 2017. https://eprint.iacr.org/2017/962.
31. A. Rostovtsev and A. Stolbunov. Public-Key Cryptosystem Based on Isogenies. *IACR Cryptol. ePrint Arch.*, 2006:145, 2006.
32. René Schoof. Nonsingular cubic curves over finite fields, November 1987. http://www.mat.uniroma2.it/~schoof/cubiccurves.pdf.
33. J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New-York, 1994.
34. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.
35. David Urbanik and David Jao. New techniques for SIDH-based NIKE. *Journal of Mathematical Cryptology*, 14(1):120–128, 2020.
36. Paul C Van Oorschot and Michael J Wiener. Parallel collision search with cryptanalytic applications. *Journal of cryptology*, 12(1):1–28, 1999.
37. Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Chapman & Hall/CRC, 2 edition, 2008.
38. Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. Cryptology ePrint Archive, Report 2021/919, 2021. https://ia.cr/2021/919.

A A simpler, but detectable variant of the attack

We present a simpler variant of our attack, but which can be easily detected. In Section 4.2, we use Algorithm 1 to recover the action of ϕ_A on groups of order

$N_B\ell^v$. In the case where ℓ is coprime to N_B, there is no need to consider groups of order $N_B\ell^v$ since we already know the action of ϕ_A on the N_B-torsion points. Therefore, we can directly recover the action of ϕ_A on groups of order ℓ^v.

Let d be the smallest divisor of N_B such that $N_B = dN'_B$ and N'_B is a square modulo N_A, say $N'_B \equiv \gamma^2 \mod N_A$. To recover the action of ϕ_A on a cyclic group G_1 of order ℓ where $\ell \equiv \mu^2 \mod N_A$, Bob chooses a cyclic group G_0 of order d and sets $G = G_0 + G_1$, which is a group of order $d\ell$. He computes the isogeny $\phi_G : E_0 \to E_G = E_0/G$ together with $R = [\gamma\mu^{-1}]\phi_G(P_A)$ $S = [\gamma\mu^{-1}]\phi_G(Q_A)$. For each cyclic group $H \subset E_A[d\ell]$ containing $\phi_A(G_0)$, Bob computes $E_H = E_A/H$ and queries the oracle (E_G, R, S, E_H). Note that

$$\begin{aligned} e_{N_A}(R,S) &= e_{N_A}([\gamma\mu^{-1}]\phi_G(P_A), [\gamma\mu^{-1}]\phi_G(Q_A)) \\ &= e_{N_A}(P_A, Q_A)^{\gamma^2\mu^{-2}\deg\phi_G} \\ &= e_{N_A}(P_A, Q_A)^{N'_B\ell^{-1}d\ell} \\ &= e_{N_A}(P_A, Q_A)^{N_B}, \end{aligned}$$

Hence the pairing check does not detect the attack. Nevertheless, when N_B is a very smooth integer (like in SIDH where $N_B = 3^b$ and $d \in \{1, \ell\}$), d is small. Hence Alice can easily check if the curves E_0 and E_G are $d\ell$-isogenous to discard such malicious public keys.