

From: (b) (6)
To: [Moody, Dustin \(Fed\)](#)
Subject: CT-RSA paper on attacks on SIDH
Date: Sunday, September 26, 2021 9:19:39 AM
Attachments: [CT-RSA 2022 paper 88 \(SIDH attack\).pdf](#)

Hi Dustin,

I'm on the PC for CT-RSA and one of the papers in my pile is about an apparently new adaptive attack on SIDH. The paper is attached below. Would you like to review it? I would need the review by October 26th.

If you're interested, let me know and I will send the official invite + review guidelines.

Thanks!
Gorjan

A New Adaptive Attack on SIDH

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 SIDH¹ 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 [27,8]. 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 [20,12] 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 Kutas et al. [22] 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 [26,10]. A rigorous proof of the equivalence between the two problems was recently proposed by Wesolowski [33].

¹ Disclaimer: this result is applicable to SIDH-type schemes only, not to SIKE.

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 through 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, these 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) [17]. 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[19] (Supersingular Isogeny Key Encapsulation), the GPST adaptive attack is avoided by leveraging SIDH with a variant [18] of the Fujisaki-Okamoto transform [14].

The first passive torsion points attacks are due to Petit [25] and were recently improved by de Quehen et al. [9]. 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 [9] is more efficient compared to the generic meet in the middle and the van-Oorschot - Wiener (vOW) attack [31]. 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 [9, Figure 1]. Other passive attacks exploiting the availability of torsion points in the public key are described in [13, 22].

The improved torsion points attacks do not apply to SIKE and BSIDH 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 $\varphi : E_0 \rightarrow E$ 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 $G_1, G_2, G_3 \subset E_0[N_B]$ 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 $\varphi_A : E_0 \rightarrow E_A$ 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 $G_1, G_3, G_3 \subset E_0[N_B]$ of order $N_B N$ 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 attack parameters for SIDH primes \$IDHp182, \$IDHp217, SIDHp377, SIDHp434, SIDHp503 and SIDHp546. For these SIDH primes, we suggest attack parameters for which the attack fully recovers Bob's secret isogeny querying a few tens of thousand times the key exchange key exchange oracle. We are currently computing the best attack parameters for BSIDH primes. We suggest countermeasures among which the Fujisaki-Okamoto transform (as used in SIKE), using SIDH proof of isogeny knowledge as recently proposed in [11] 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 [9, §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 suffice 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 \mathbf{F}_q , the set of \mathbf{F}_q -rational points $E(\mathbf{F}_q)$ 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 $\mathbf{Z}_N \oplus \mathbf{Z}_N$.

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 V'elu's formulas [29] 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.

2.2 SIDH: Supersingular Isogeny Diffie-Hellman

The SIDH scheme is defined as follows.

Setup. Let $p = \#E_A \#E_B - 1$ be a prime such that $\#E_A \approx \#E_B \approx \sqrt{p}$. Let E_0 be a supersingular curve defined over \mathbf{F}_{p^2} . Set $E_0[\mathcal{E}_A] = (P_A, Q_A)$ and $E_0[\mathcal{E}_B] = (P_B, Q_B)$. The public parameters are $E_0, p, \mathcal{E}_A, \mathcal{E}_B, e_A, e_B, P_A, Q_A, P_B, Q_B$.

KeyGeneration. The secret key sk_A of Alice is a uniformly random integer a sampled from $\mathbf{Z}_{\#E_A}$. Compute the cyclic isogeny $\varphi_A : E_0 \rightarrow E_A = E_0 / (P_A + [a]Q_A)$. The public key of Alice is the tuple $pk_A = (E_A, \varphi_A(P_B), \varphi_A(Q_B))$. Analogously, Bob's secret key sk_B is a uniformly random integer β sampled from $\mathbf{Z}_{\#E_B}$ and his public key is $pk_B = (E_B, \varphi_B(P_A), \varphi_B(Q_A))$ where $\varphi_B : E_0 \rightarrow E_B = E_0 / (P_B + [\beta]Q_B)$.

KeyExchange. Upon receiving Bob's public key (E_B, R_a, S_a) , Alice checks that $e(R_a, S_a) = e(P_A, Q_A)^{e_B}$, if not she aborts. She computes the isogeny $\varphi^* : E_B \rightarrow E_{BA} = E_B / (R_a + [a]S_a)$. Her shared key is $j(E_{BA})$. Similarly, upon receiving (E_A, R_b, S_b) , Bob checks that $e(R_b, S_b) = e(P_B, Q_B)^{e_A}$, if not he aborts.

He computes the isogeny $\varphi^* : E_A \rightarrow E_{AB} = E_A / (R_b + [\beta]S_b)$. His shared key is $j(E_{AB})$.

The correctness of the key exchange follows from the fact that

$$E_A / (\varphi_A(P_B) + [\beta]\varphi_A(Q_B)) \simeq E_0 / (P_A + [a]Q_A, P_B + [\beta]Q_B) \simeq E_B / (\varphi_B(P_A) + [\alpha]\varphi_B(Q_A)) .$$

The scheme is summarized in Figure 1.

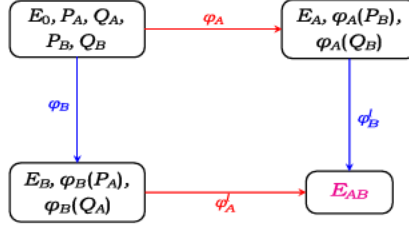


Fig. 1: SIDH Key Exchange

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 $E_0, P_A, Q_A, P_B, Q_B, E_A, \varphi_A(P_B), \varphi_A(Q_B), E_B, \varphi_B(P_A), \varphi_B(Q_A)$ (defined as in SIDH), compute E_{AB} .

Problem 2 (Supersingular Isogeny Decisional Diffie-Hellman). Given $E_0, P_A, Q_A, P_B, Q_B, E_A, \varphi_A(P_B), \varphi_A(Q_B), E_B, \varphi_B(P_A), \varphi_B(Q_A)$ (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 [12] one does a pairing-based check on the torsion points $\varphi_B(P_A)$ and $\varphi_B(Q_A)$ 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. Let $e_N : E[N] \times E[N] \rightarrow \mu_N$ be the Weil pairing [16]. Let $\varphi : E \rightarrow E^\sharp$ be an isogeny of degree M , then for $P, Q \in E[N]$,

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

where the first pairing is computed on E^\sharp and the second one on E . In SIDH, given (E_B, R, S) returned by Bob as public key, Alice checks if

$$e_{f_A^A}(R, S) = e_{f_A^A}(P_A, Q_A)^{e_B^B}.$$

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 [17] is that if Bob manipulates the torsion points $\varphi_B(P_A)$ and $\varphi_B(Q_A)$

conveniently, then he can get some information about Alice's private key a 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:

$O(E, R, S, E^*)$ which returns 1 if $j(E^*) = j(E / (R + [a]S))$ and 0 otherwise

If one supposes that $\mathcal{E}_A = 2$ and $e_A = n$, then after each query, Bob recovers one bit of

$$a = a_0 + 2^1 a_1 + 2^2 a_2 + \dots + 2^{n-1} a_{n-1}.$$

Concretely, let us suppose that Bob has successfully recovered the first i bits of a , say $K_i = a_0 + 2^1 a_1 + \dots + 2^{i-1} a_{i-1}$ so that

$$a = K_i + 2^i a_i + 2^{i+1} a^t$$

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

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

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

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

where $\theta = \frac{1}{(1 + 2^{n-i-1})^{-1}}$. The attack recovers the first $n-2$ bits of a using $n-2$ oracle queries, and it recovers the two remaining bits by brute force. We refer to [17] 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 Problem 3.

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 *Supersingular Isogeny Problem*.

Problem 3. 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 \mathbf{F}_{p^2} . Set $E_0[N_B] = \{P, Q\}$ and let $\varphi : E_0 \rightarrow E$ be a random isogeny of degree A . Given $E_0, E, P, Q, \varphi(P)$ and $\varphi(Q)$, 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 [25] 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. [9].

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

$$N_A^2 \deg \theta + d^2 = N_B^2 e. \quad (1)$$

Writing Equation 1 in terms of isogenies we get

$$\varphi \circ \theta \circ \varphi + [d] = \psi_1 \circ \psi_e \circ \psi_2 \quad (2)$$

where ψ_1 and ψ_2 are isogenies of degree N_B , ψ_e is an isogeny of degree e . The torsion point information $\varphi(P), \varphi(Q)$ is used to evaluate $\tau = \varphi \circ \theta \circ \varphi + [d]$ on $E[N_B]$. Knowing τ on $E_0[N_B]$, the kernels of the isogenies $\varphi_1 : E \rightarrow E_1$ and $\varphi_2 : E \rightarrow E_2$ can be recovered efficiently. The isogeny $\psi_e : E_1 \rightarrow E_2$ is recovered by brute force or meet in the middle. We refer to [9, § 4.1] for technical details.

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

$$\ker \varphi = \ker (\psi_1 \circ \psi_e \circ \psi_2 - [d]) \cap E[N_A].$$

Figure 2 illustrates the attack.

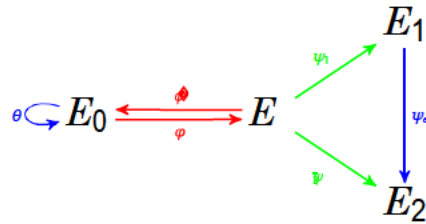


Fig. 2: Improved torsion points attack.

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. [9] 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: $N_B > \sqrt[p]{pN_A}$;
3. Superpolynomial time but asymptotically more efficient than quantum claw-finding [21] when: $N_B > \max\{A, \sqrt[p]{p}\}$.

More concretely, if $N_A \approx p^a$ and $N_B \approx N_A p^\eta$, then the improved torsion points attack runs in time $\tilde{O}\left(N^{\frac{1+2(a-\eta)}{4}}\right)$ and $\tilde{C}\left(N^{\frac{1+2(a-\eta)}{8}}\right)$ on a classical computer and a quantum computer respectively [9, §6.2 Proposition 27]. In the special case where $a = \frac{1}{2}$, 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, [9, Algorithm 7] solves Problem 3 in polynomial time.*

Remark 1. SIKE parameters (for which E_0 is close to a curve having j -invariant 1728 and $N_A \approx N_B \sqrt[p]{p}$) 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 \mathbf{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 $\varphi : E_0 \rightarrow E$ be a random isogeny of degree N_A .

Given $E_0, G_1, G_2, G_3, E, \varphi(G_1), \varphi(G_2)$ and $\varphi(G_3)$, 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 $\tau = \varphi \circ \theta \circ \varphi + [d]$. Let G_1, G_2 and G_3 be as in Problem 4. In the improved torsion point attacks, the torsion point information $(\varphi(P), \varphi(Q))$ 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 $\varphi(G_1)$, $\varphi(G_2)$ and $\varphi(G_3)$ 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 $[\lambda] \circ \varphi$ for some integer λ coprime to N_B . Concretely, we have the following lemma.

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

The result in Lemma 1 is 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 $[\lambda] \circ \varphi$ on the N_B torsion for some $\lambda \in (\mathbf{Z}/N_B\mathbf{Z})^\times$ 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 $x^2 \equiv a^2 \pmod{N_B}$ have more than two solutions.

Proof (of Lemma 1). For $i = 1, 2, 3$, set $\varphi(P_i) = [\lambda_i]Q_i$ where $\lambda_i \in (\mathbf{Z}/N_B\mathbf{Z})^\times$. 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

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

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 is coprime to d , then $H_1 \cap H_3 = H_2 \cap H_3 = \{0\}$ and $u_1, u_2, v_1, v_2 \in (\mathbf{Z}/N_B\mathbf{Z})^\times$. Thus $\lambda_1 v_1 / u_1 = \lambda_3 = \lambda_2 v_2 / u_2$, and $\varphi(P_1) = [\lambda_3]Q_1^t$, $\varphi(P_2) = [\lambda_3]Q_2^t$ where $Q_1^t = [v_1 / u_1]Q_1$ and $Q_2^t = [v_2 / u_2]Q_2$.

We have

$$e_N(P_1, P_2)^{\deg \varphi} = e_N(\varphi(P_1), \varphi(P_2)) = e_N([\lambda_3]Q_1^t, [\lambda_3]Q_2^t) = e_N(Q_1^t, Q_2^t)^{\lambda_3^2}.$$

We recover λ_3^2 by solving the following discrete logarithm

$$\lambda_3^2 = DLP \left(e_N(P_1, P_2)^{\deg \varphi}, e_N(Q_1^t, Q_2^t) \right).$$

For any $S = [a]P_1 + [\beta]P_2 \in E_0[N_B]$ we have $[\lambda_3] \circ \varphi(S) = [a]Q_1^t + [\beta]Q_2^t$. \square

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

Since we can evaluate $\varphi_\lambda = [\lambda] \circ \varphi$ on $E_0[N_B]$, then we can evaluate φ_λ on $E[N_B]$ as well. Therefore we can evaluate $\varphi_\lambda \circ \theta \circ \varphi$ on $E[N_B]$. Meanwhile, we have

$$\varphi_\lambda \circ \theta \circ \varphi = ([\lambda] \circ \varphi) \circ \theta \circ ([\lambda] \circ \varphi) = [\lambda^2] \circ \varphi \circ \theta \circ \varphi.$$

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

$$\varphi \circ \theta \circ \varphi^\diamond = [\lambda^2] \circ \varphi_A \circ \theta \circ \varphi_A$$

on $E[N_B]$. Hence $\tau = \varphi \circ \theta \circ \varphi^\diamond [d]$ can be efficiently evaluated on $E[N_B]$. This concludes our discussion.

From now on, we can translate the solutions in [9] 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 $\theta \in \text{End}(E_0)$ to $E_0[N_B]$, an integer d coprime to N_B , and a smooth integer e such that*

$$\deg \varphi \circ \theta \circ \varphi^\diamond + [d] = N_B e \quad \text{or} \quad \deg \varphi \circ \theta \circ \varphi^\diamond + [d] = N_B p e.$$

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

Proof. Follows from the previous discussion, [9, Theorem 3] and [9, Theorem 5].

We have the following Corollary.

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

In the following section, we use the revisited 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, $E_0[N_B] = (P_B, Q_B)$, and let $(E_A, \varphi_A(P_B), \varphi_A(Q_B))$ be Alice's public key where her static secret key is an isogeny $\varphi_A : E_0 \rightarrow E_A$ of degree N_A . Moreover, suppose that you are given some "suitable" N -smooth integer N coprime to N_A such that $E_0[N_B N] \subset E_0(\mathbf{F}_{p^{2k}})$ 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 $(E_A, \varphi_A(P_B), \varphi_A(Q_B))$ into a tuple $(E_A, \varphi_A(G_1), \varphi_A(G_2), \varphi_A(G_3))$ where $G_1 = (P)$, $G_2 = (Q)$, $G_3 = (R)$ are cyclic subgroups of maximal order in $E_0[N_B N]$, such that $G_1 \cap G_2 \cap G_3 = \{O\}$.
- **The passive phase.** Having $(E_A, \varphi_A(G_1), \varphi_A(G_2), \varphi_A(G_3))$, 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 $N = \mathcal{E}^{v_1} \cdot \dots \cdot \mathcal{E}_n^{v_n}$ be a smooth integer coprime to N_A such that $E_0[\mathcal{E}_i^{v_i}] \subset E(\mathbf{F}_{p^{2k}})$ and for each prime \mathcal{E}_i which is not a square modulo N_A , v_i is even. Let G_1, G_2, G_3 are cyclic subgroups of $E_0[N_B N]$ order $N_B N$ such that $G_1 \cap G_2 \cap G_3 = \{O\}$. The active phase of the attack consists in recovering $\varphi_A(G_j)$ for $j = 1, 2, 3$.

For $j = 1, 2, 3$, we can represent G_j as $G_j = \bigcup_{i=1}^r G_{ji}$ where G_{ji} is a group of order $N_B \mathcal{E}_i^{v_i}$. The action of φ_A on G_j is recovered by computing $\varphi_A(G_{ji})$ for $i = 1, \dots, n$. Storing $\varphi_A(G_j)$ in this form enables us to perform all computations in extension fields of degree k_1, \dots, k_n , instead of $LCM(k_1, \dots, k_n)$ the full group G_j is considered. This is because all supersingular isogenies are \mathbf{F}_{p^2} -rational. Hence we never go to extension fields with degree beyond $\max\{k_i, i = 1, \dots, n\}$. Let us describe how we compute $\varphi_A(G_{ji})$ for $j = 1, 2, 3$ and $i = 1, \dots, n$.

Let G be a cyclic subgroup of $E_0[N_B \mathcal{E}^v]$ of order $N_B \mathcal{E}^v$. Let us suppose that \mathcal{E} is a square modulo N_A and that $v = 1$. Note that $\varphi_A([\mathcal{E}]G)$ 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 $N_B \mathcal{E}$, Bob computes the isogeny $\varphi_G : E_0 \rightarrow E_G$ having kernel G together with $R = [\mu^{-1}]\varphi_G(P_A)$, $S = [\mu^{-1}]\varphi_G(Q_A)$. Let H be a random cyclic subgroup of $E_A[N_B \mathcal{E}]$ of order $N_B \mathcal{E}$ containing $\varphi_A([\mathcal{E}]G)$. Let $\varphi_H : E_A \rightarrow E_H$ be the isogeny of kernel H and $\varphi_A^* : E_G \rightarrow E_G/\varphi_G(\ker(\varphi_A))$ be the isogeny of kernel $\varphi_G(\ker(\varphi_A))$. Then if H is the image of the group G through φ then the diagram in Figure 3 commutes and $O(E_G, R, S, E_H) = 1$. In the other case, when $H = \varphi_A(G)$, Lemma 2 shows that the oracle returns 1 with negligible probability.

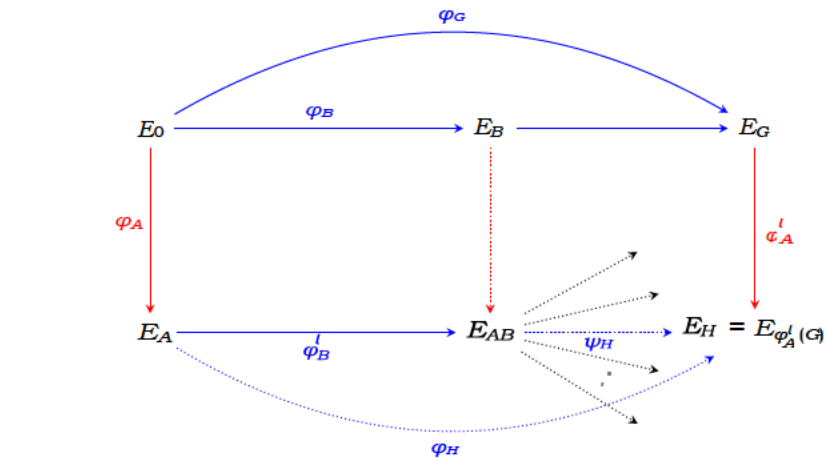


Fig. 3: Computing the action of φ_A on G .

Lemma 2. Suppose that $\mathfrak{E} \approx O(\log p)$ and $N_A N_B \approx p$ (or $N_A N_B > p$), and let G, H, E_H and $E_G/\varphi_G(\ker(\varphi_A))$ be defined as above. If $H \neq \varphi_A(G)$ the $E_H = E_G/\varphi_G(\ker(\varphi_A))$ with negligible probability.

Proof. Let $H^\sharp = \varphi_A(G)$. By construction, we get $[\mathcal{E}]H = [\mathcal{E}]\varphi_A(G) = [\mathcal{E}]H^\sharp$, and we can decompose φ_H and φ_H^\sharp as $\varphi_H = \psi_H \circ \varphi_B^\sharp$ and $\varphi_H^\sharp = \psi_H^\sharp \circ \varphi_B^\sharp$ where φ_H and φ_H^\sharp are isogenies of degree \mathcal{E} from E_{AB} to $E_G/\varphi_G(\ker(\varphi_A))$. Since $H \neq H^\sharp$, then $\psi_H^\sharp = \pm \psi_H$ and $\psi_H^\sharp - \psi_H$ is a non scalar endomorphism of E_{AB} of degree \mathcal{E}^2 . Therefore, the curve E_{AB} is an \mathcal{E}^2 -small curve as defined in [24].

On the other hand, since $N_{ANB} \approx p$, then E_{AB} is statistically a random supersingular curve since. Moreover, the number of \mathcal{E} -small curves is roughly \mathcal{E}^3 [24]. Considering the fact that the number of supersingular curves defined over \mathbf{F}_{p^2} is $\frac{p-1}{12}$, then the probability that E_{AB} is an \mathcal{E} -small curve is at roughly $\frac{12\mathcal{E}^3}{p}$, which is negligible since $\mathcal{E} \approx O(\log p)$. \square

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

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

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

If $1 < \nu$, then the process can be iterated to recover the action of φ_A on groups of order $N_{B\mathcal{E}}, N_{B\mathcal{E}^2}, \dots, N_{B\mathcal{E}^\nu}$ when \mathcal{E} is a square modulo N_A , respectively $N_{B\mathcal{E}^2}$,

$N_B\mathcal{E}^4, \dots, N_B\mathcal{E}^v$ when \mathcal{E} 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 .

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

Require: $E_0, P_A, Q_A, P_M, Q_M, E_A, \varphi_A(P_B), \varphi_A(Q_B), G$.

Ensure: $\varphi_A(G)$.

```

1: Set  $G_0 = [\mathcal{E}^v]G$ ;
2: if  $\mathcal{E}$  is a square modulo  $N_A$  then
3:   Compute  $\mu = \mathcal{E} \bmod N_A$ ;
4:   for  $i = 1, \dots, v$  do
5:      $G_i = [\mathcal{E}^{v-i}]G$ 
6:     Compute  $\varphi_{G_i} : E_0 \rightarrow E_{G_i}$  of degree  $N_B\mathcal{E}^i$  and of kernel  $G_i$ , together
       with  $R = [\mu^{-i}]\varphi(P_A)$  and  $S = [\mu^{-i}]\varphi(Q_A)$ ;
7:     for  $H$  cyclic group of  $E_A$  of order  $N_B\mathcal{E}^i$  containing  $\varphi_A(G_{i-1})$  do
8:       Compute  $\varphi_H : E_A \rightarrow E_H$  of kernel  $H$ ;
9:       if  $O(E, R, S, E_H) = 1$  then
10:        Set  $\varphi_A(G_i) = H$ ;
11:    $G^* = \varphi_A(G_v)$ ;
12: else
13:   for  $i = 1, \dots, v/2$  do
14:      $G_i = [\mathcal{E}^{v-2i}]G$ 
15:     Compute  $\varphi_{G_i} : E_0 \rightarrow E_{G_i}$  of degree  $N_B\mathcal{E}^{2i}$  and of kernel  $G_i$ , together
       with  $R = [\mathcal{E}^{-i}]\varphi(P_A)$  and  $S = [\mathcal{E}^{-i}]\varphi(Q_A)$ ;
16:     for  $H$  cyclic group of  $E_A$  of order  $N_B\mathcal{E}^{2i}$  containing  $\varphi_A(G_{i-1})$  do
17:       Compute  $\varphi_H : E_A \rightarrow E_H$  of kernel  $H$ ;
18:       if  $O(E, R, S, E_H) = 1$  then
19:        Set  $\varphi_A(G_i) = H$ ;
20:    $G^* = \varphi_A(G_{v/2})$ ;
21: return  $G^*$ .
```

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

Proof. Since \mathcal{E} , 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 $O(k_v \cdot \text{poly}(\log p))$. The second point of the Lemma follows from Lemma 2. \square

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

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

Require: $E_0, P_A, Q_A, P_B, Q_B, E_A, \varphi_A(P_B), \varphi_A(Q_B), N_A, N_B, N = \mathfrak{L}_1^{\nu_1} \cdots \mathfrak{L}_n^{\nu_n},$

G_{ji} for $j = 1, 2, 3$ and $i = 1, \dots, n.$

Ensure: $\varphi_A(G_{ji})$ for $j = 1, 2, 3$ and $i = 1, \dots, r.$

```

1: for  $i = 1, \dots, n$  do
2:   for  $j = 1, 2, 3$  do
3:     Compute  $\varphi_A(G_{ji})$  using Algorithm 1;
4: return  $\varphi_A(G_{ji})$  for  $j = 1, 2, 3$  and  $i = 1, \dots, n.$ 

```

Lemma 4. *Algorithm 2 runs in time $\tilde{O}(\max\{k^*\})$ whenever \mathfrak{L}_i for $i = 1, \dots, n$, 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 .

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 $N = \mathfrak{L}_1^{\nu_1} \cdots \mathfrak{L}_n^{\nu_n}$ coprime to N_A such that $E_0[N_B \mathfrak{L}_i^{\nu_i}] \subset E(\mathbf{F}_{p^{2k}})$ and for each prime \mathfrak{L}_i which is not a square modulo N_A , ν_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/\mathbf{F}_{p^2} be a supersingular elliptic curve such that $E(\mathbf{F}_{p^2}) \sim (\mathbf{Z}_{p-E})$ where $E = \pm 1$ corresponds to the sign of the trace of Frobenius $t = 2Ep$ of E over \mathbf{F}_{p^2} . Then for every natural number k , the group structure of E over $\mathbf{F}_{p^{2k}}$ is given by*

$$E(\mathbf{F}_{p^{2k}}) \sim (\mathbf{Z}_{p^k - E^k})^2 \quad (3)$$

Proof. Let k be natural number and let t_k be the trace of Frobenius of E over $\mathbf{F}_{p^{2k}}$. Then by Hasse Theorem (theorem V.1.1 of [29]),

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

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

$$X^2 - 2EpX + p^2 = (X - Ep)^2$$

By Theorem 4.12 of [32]

$$t_k = 2(Ep)^k = 2E^k p^k$$

where E^k is the sign of t_k . Hence $t_k^2 = 4p^{2k}$ and by lemma 4.8 of [28]

$$E(\mathbf{F}_{p^{2k}}) \sim (\mathbf{Z}^{\sqrt{\frac{p^{2k}}{r^{2k}-E^k}}})^2 \sim (\mathbf{Z}_{p^k-E^k})^2.$$

□

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

Let \mathcal{E} be a small prime. Then $\mathcal{E}^v | p^{2k} - 1$ for some $k \leq \mathcal{E}^v$. This means that for each prime \mathcal{E}_i dividing N , $k_i \leq \mathcal{E}_i^{v_i}$. This leads to a easy way to compute N : choose the smallest primes \mathcal{E}_i coprime to $N_A N_B$, such that $p < N = \mathcal{E}_i^2$ let $N = \mathcal{E}_i^2 = p^{1+E}$ with $E > 0$. Then the largest \mathcal{E}_i is in $O(\log p)$. Moreover we have k_i at most \mathcal{E}_i^2 .

To moderate the fields extension degrees, we also include in N primes \mathcal{E} that are squares modulo N_A . For this primes, we only require \mathcal{E} 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.

Algorithm 3 Computing N

Require: p, N_A, N_B .

Ensure: P, D .

```

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

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

Proof. Follows from the previous discussion. □

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, one may set a bound on the extension degrees and slightly increase the size of the primes \mathcal{E}_i . This will be the case in the attack parameters we will present in Section 5.

4.4 Attack summary

The full attack can be summarised in Algorithm 4.

Algorithm 4 New Adaptive attack on SIDH

Require: $E_0, P_A, Q_A, P_B, Q_B, E_A, \varphi_A(P_B), \varphi_A(Q_B), N_A, N_B$.

Ensure: $\ker(\varphi_A)$.

- 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 $\varphi_A(G_1), \varphi_A(G_2), \varphi_A(G_3)$ 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** $\ker(\varphi_A)$.
-

Now we evaluate the number of oracle queries. Since $N = \mathcal{E}_1^{v_1} \cdots \mathcal{E}_n^{v_n}$ where for each prime \mathcal{E}_i which is not a square modulo N_A , v_i is even, then we can write $N = \mathcal{E}_1^{2v_1} \cdots \mathcal{E}_n^{2v_n} \mathcal{E}_{n+1}^{u_1} \cdots \mathcal{E}_{n+m}^{u_m}$ where the primes \mathcal{E}_{n+j} for $j = 1, \dots, m$ are squares modulo N_A . From Algorithm 1, for each prime factor \mathcal{E}_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 $(\mathbf{Z}/\mathcal{E}_i^2 \mathbf{Z})^2$ order \mathcal{E}_i^2 , which is $\mathcal{E}_i(\mathcal{E}_i + 1)$. Note that if the first $\mathcal{E}_i(\mathcal{E}_i + 1) - 1$ queries fail, then there is no need to perform the last query since it will succeed. Also, for each prime factor \mathcal{E}_{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 $(\mathbf{Z}/\mathcal{E}_i \mathbf{Z})^2$ order \mathcal{E}_i , which is $\mathcal{E}_i + 1$. Here also, there is no need to perform the last query when the first \mathcal{E}_i queries failed. Therefore, the maximum number of oracle queries in the attack is

$$O_q = \sum_{i=1}^n v_i [\mathcal{E}_i(\mathcal{E}_i + 1) - 1] + \sum_{j=1}^m u_j \mathcal{E}_{n+j}.$$

Now we can state the main result of this paper.

Theorem 2. Let $p, E_0, N_A < p, N_B < p, P_A, Q_A, P_B, Q_B, E_A, \varphi_A(P_B), \varphi_A(Q_B)$ 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

$$O_q = \sum_{i=1}^n v_i [\mathcal{E}_i(\mathcal{E}_i + 1) - 1] + \sum_{j=1}^m u_j \mathcal{E}_{n+j}$$

queries to the key exchange oracle $N = \mathbb{F}_1^{2v_1} \cdots \mathbb{F}_n^{2v_n} \mathbb{F}_{n+1}^{u_1} \cdots \mathbb{F}_{n+m}^{u_m}$ is the integer computed in Step 1.

Proof. By Lemma 3, Step 1 outputs a smooth integer N such that $\max k_i \leq O(\log^2 p)$. 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. \square

5 Relevance and countermeasures

In this section, we suggest some attack parameters for \$IDHp, SIDH and BSIDH parameters. 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 [7, §10], the SIDH primes SIDHp377 and SIDHp546 suggested by Longa et. al [23], SIDHp434 and SIDHp503 as specified in SIKE [19].

As attack parameters, we provide the prime factorisation of N , the maximum field extension degree $k^* = \max k_i$, $\eta = N/p$ 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
SIDHp182 prime: $p = 2^{91}3^{57} - 1$				
B	96	$\frac{185}{182}$	7251	$5^2 * 7 * 11^2 * 13 * 19 * 31 * 37 * 43 * 47^2 * 61 * 67 * 73 * 79 * 97 * 103 * 109 * 127 * 139 * 157 * 181 * 241 * 277 * 421 * 433 * 541 * 661 * 919$
SIDHp217 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.

Remark 5. 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 [30]. In the later case, the number of oracle queries is exponential in k .

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.

5.2 Countermeasures to the attack

A straightforward countermeasure of the attack is to use a variant of the Fujisaki-Okamoto transform [15,18] 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 [11]. 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\$, \$IDHp377\$, \$IDHp434\$, \$IDHp546\$ and \$IDHp503\$. 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 [11] 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.

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. 17
2. Andrea Basso, Peter 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>. 9
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
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>. 17
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. 1
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. 1
7. 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>. 17

8. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. <https://eprint.iacr.org/2006/291>. 1
9. Victoria de Quehen, P'eter 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>. 2, 3, 7, 8, 10
10. Kirsten Eisentra"ger, 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. 1
11. 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>. 3, 18, 19
12. Luca De Feo, David Jao, and J'ero"me Pl"ut. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, 2014. Pagesn 209-247. 1, 5
13. Tako Boris Fouotsa, P'eter 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>. 2
14. Eiichi 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. 2
15. Eiichi Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Annual International Cryptology Conference*, pages 537–554. Springer, 1999. 18
16. Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. 5
17. 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. 2, 5, 6
18. Dennis Hofheinz, Kathrin Ho"velmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017. 2, 18
19. 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>. 2, 17
20. 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. 1
21. Samuel Jaques and Andr'e Schrottenloher. Low-gate quantum golden collision finding. Cryptology ePrint Archive, Report 2020/424, 2020. <https://eprint.iacr.org/2020/424>. 8
22. P. Kutas, Simon-Philipp Merz, C. Petit, and Charlotte Weitka"mper. One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols. *IACR Cryptol. ePrint Arch.*, 2021:282, 2021. 1, 2
23. 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>. 17

24. Jonathan Love and D. Boneh. Supersingular curves with small non-integer endomorphisms. *ArXiv*, abs/1910.03180, 2019. 12
25. 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. 2, 7
26. 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>. 1
27. A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptol. ePrint Arch.*, 2006:145, 2006. 1
28. Ren e Schoof. Nonsingular cubic curves over finite fields, November 1987. <http://www.mat.uniroma2.it/~schoof/cubiccurves.pdf>. 15
29. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009. 4, 14
30. David Urbanik and David Jao. New techniques for SIDH-based NIKE. *Journal of Mathematical Cryptology*, 14(1):120–128, 2020. 17
31. Paul C Van Oorschot and Michael J Wiener. Parallel collision search with cryptanalytic applications. *Journal of cryptology*, 12(1):1–28, 1999. 2
32. Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Chapman & Hall/CRC, 2 edition, 2008. 14
33. Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. Cryptology ePrint Archive, Report 2021/919, 2021. <https://ia.cr/2021/919>. 1