# On weak keys of POKÉ

Tomoki Moriya

Information Technology R&D Center, Mistubishi Electric Corporation, Japan
Moriya.Tomoki@bp.MitsubishiElectric.co.jp

**Abstract.** POKÉ is an isogeny-based public-key encryption (PKE) scheme proposed by Basso and Maino. Among existing isogeny-based PKE schemes, POKÉ is known to achieve relatively high performance. However, the security of POKÉ relies on certain ad hoc assumptions, and its security analysis may not yet be fully comprehensive.
In this work, we investigate the security of POKÉ. We show that POKÉ admits *weak keys* that reduce the complexity of certain attacks. In the POKÉ-2D setting, these weak keys do not significantly affect the overall security, since the probability that such keys occur is sufficiently small. In contrast, we demonstrate that POKÉ-4D is threatened by the presence of these weak keys.
Finally, we suggest novel parameters for POKÉ-4D in order to mitigate the aforementioned weak-key attack. The resulting parameter sizes are comparable to those of POKÉ-2D. Consequently, the principal advantages of POKÉ-4D in terms of performance—namely, a more compact prime size and a more efficient encryption algorithm—are no longer preserved.

## 1 Introduction

Isogeny-based cryptography is one of the promising candidates for post-quantum cryptography, which is based on the Isogeny problem of supersingular elliptic curves. A notable feature of isogeny-based cryptosystems is that they achieve relatively compact key sizes. In particular, SQISign [11,1], which remains a candidate in the NIST Post-Quantum Cryptography Standardization Process for additional digital signatures [21], achieves the smallest signature size among all candidates in the standardization process. However, there are several hurdles that prevent isogeny-based cryptosystems from being deployed in the real world. In particular, the following two issues are frequently cited:

- isogeny-based cryptosystems are relatively inefficient; and
- the security analysis of isogeny-based cryptographic schemes remains insufficient.

SIDH was an isogeny-based key exchange scheme proposed in [15,10], which was regarded as a compact and efficient isogeny-based protocol. However, subsequent cryptanalytic work has shown that SIDH can be broken in polynomial time via torsion-point attacks and higher-dimensional isogeny techniques [7,19,22].

Surprisingly, the attacks described above have also led to novel computational techniques in isogeny-based cryptography that enable several promising new constructions. For example, SQISignHD [9] is the first application of the SIDH attack and yields more compact signatures than the original SQISign. Another example is FESTA [3], an isogeny-based public key encryption scheme that leverages the SIDH attack as a constructive trapdoor mechanism. These and related schemes have inspired a variety of high-performance isogeny-based primitives. However, they typically rely on non-standard or ad hoc security assumptions, and there remains concern that they may ultimately be vulnerable to attacks analogous to those that broke SIDH.

POKÉ is an isogeny-based public key encryption scheme proposed by Basso and Maino [2]. POKÉ is one of isogeny-based schemes using the SIDH attack, and achieves high performance among isogeny-based public-key encryption schemes, in the sense that it realizes compact key sizes and enables efficient encryption and decryption.

As with other isogeny-based schemes, one disadvantage of POKÉ is that its security relies on a novel mathematical problem: a variant of the isogeny problem endowed with torsion-point information in which the degree of the hidden isogeny is masked. To the best of our knowledge, there are no known results addressing this problem, which raises concerns regarding the security of POKÉ. Moreover, POKÉ employs a structure similar to that of SIDH, which can be broken in polynomial-time as we already mentioned. Consequently, further security analysis of POKÉ is essential for its prospective deployment in real-world applications.

### 1.1 Contribution

In this study, we analyze the security of POKÉ. More precisely, we first define a mathematical problem, called the Masked-degree Isogeny problem with torsions (Definition 6), which is closely related to the security of POKÉ, and then analyze the hardness of this problem.

Our main contributions are summarized as follows.

- We show that a random instance of the Masked-degree Isogeny problem with torsion can be solved in polynomial time with probability $O(1/\sqrt{\delta_{\mathsf{m}}})$, where $\delta_{\mathsf{m}}$ is the upper bound of the degrees of secret isogenies, set to $\delta_{\mathsf{m}} \approx 2^{2\lambda}$ in POKÉ-2D and $\delta_{\mathsf{m}} \approx 2^{\lambda}$ in POKÉ-4D.
- We further show that a random instance of the Masked-degree Isogeny problem with torsions can be solved in $\tilde{O}(n)$ time with probability $O(\sqrt{n/\delta_{\mathsf{m}}})$ for any $n = 1, \ldots, \delta_{\mathsf{m}}$. This result implies that, whereas POKÉ-2D can achieve $\lambda$-bit security, POKÉ-4D (and related schemes as Snake Mackerel [14] and INKE [17]) may require modification in order to attain $\lambda$-bit security.
- We finally propose new parameters for POKÉ-4D that are resistant to our weak-key attack. In particular, we recommend setting $\delta_{\mathsf{m}} \approx 2^{2\lambda}$ for POKÉ-4D. Under this choice, the performance advantages of POKÉ-4D relative to POKÉ-2D unfortunately disappear.

Our key observation is that the Masked-degree Isogeny problem with torsions can be solved in polynomial time if the secret isogeny $\phi$ satisfies

$$D'^2 - \deg\phi = r \cdot c^2,$$

where $D'$ is the order of the given torsion points, $r$ is a known integer, and $c$ is an *unknown* integer. Then, by constructing a set $\mathcal{R}$ of certain square-free integers and checking whether the problem can be solved for each $r \in \mathcal{R}$, we can attack a random instance of POKÉ in time $\tilde{O}(\#\mathcal{R})$ with some probability. After optimizing this attack, we conclude that a random instance of POKÉ can be broken in time $\tilde{O}(\#\mathcal{R})$ with probability $O(\sqrt{\#\mathcal{R}/\delta_{\mathsf{m}}})$, which implies that the parameters of POKÉ-4D should be chosen appropriately to prevent our weak-key attack.

## 2 Preliminaries

### 2.1 Elliptic curves and isogenies

We now review some mathematical background on elliptic curves and isogenies, with particular emphasis on topics relevant to isogeny-based cryptography. For further details on elliptic curves and isogenies, we refer the reader to [23].

Let $k$ be a field. An *elliptic curve defined over* $k$ is a smooth projective curve over $k$ together with a compatible group law.

For a positive integer $n$, the *$n$-torsion subgroup* of an elliptic curve $E$, denoted by $E[n]$, is defined by

$$E[n] := \{P \in E(\overline{k}) \mid nP = 0\},$$

where $\overline{k}$ denotes an algebraic closure of $k$. If $\mathrm{char}(k)$ is coprime to $n$, then there is an isomorphism of abelian groups

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

If $\mathrm{char}(k) = p > 0$, then one has either

$$E[p] \cong \mathbb{Z}/p\mathbb{Z} \quad \text{or} \quad E[p] = \{0\}.$$

We say that $E$ is an *ordinary elliptic curve* if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$; otherwise, we call $E$ a *supersingular elliptic curve*.

An *isogeny $\phi$ defined over $k$* is a morphism of elliptic curves $\phi\colon E \to E'$ defined over $k$ which is also a group homomorphism and has finite kernel.

Such an isogeny induces a homomorphism of function fields

$$\phi^*\colon k(E') \longrightarrow k(E), \qquad f \longmapsto f \circ \phi,$$

where $k(E)$ and $k(E')$ denote the function fields of $E$ and $E'$, respectively. The *degree* of $\phi$, denoted by $\deg\phi$, is defined as the degree of the field extension $[k(E) : \phi^*(k(E'))]$.

For any isogeny $\phi\colon E \to E'$, there exists a unique isogeny $\hat{\phi}\colon E' \to E$ such that

$$\hat{\phi} \circ \phi = [\deg \phi] \quad \text{and} \quad \phi \circ \hat{\phi} = [\deg \phi],$$

where $[n]$ denotes the multiplication-by-$n$ map. The isogeny $\hat{\phi}$ is called the *dual isogeny* of $\phi$.

If $\deg \phi = \#\ker \phi$, then $\phi$ is said to be a *separable isogeny*. Conversely, for any finite subgroup $G \subset E$, there exists a separable isogeny $\phi\colon E \to E'$ such that $\ker \phi = G$. The elliptic curve $E'$ is uniquely determined up to isomorphism, and we often denote a representative of its isomorphism class by $E/G$.

A separable isogeny $\phi\colon E \to E/G$ with $\ker \phi = G$ can be explicitly computed from the data $(E, G)$ in time complexity $O(\#G)$ using Vélu's formulas [24], or in time $\tilde{O}(\sqrt{\#G})$ using square-root Vélu's formulas [4].

We have the following computational problem related to isogenies.

**Definition 1 (Isogeny problem).** *Let $E$ and $E'$ be isogenous elliptic curves over a finite field of characteristic $p$.*

*The Isogeny problem is the following computational problem:*

*Given $(E, E')$, compute an isogeny $\phi\colon E \to E'$.*

The Isogeny problem is widely believed to be computationally hard, even for quantum computers, particularly in the case where $E$ and $E'$ are supersingular elliptic curves.

To the best of our knowledge, the fastest known classical algorithm for solving the Isogeny problem in the supersingular case has time complexity $\tilde{O}(p^{1/2})$ [12], while the fastest known quantum algorithm achieves complexity $\tilde{O}(p^{1/4})$ [5].

### 2.2 Kani's lemma and the SIDH attack

We next introduce Kani's lemma and a corresponding algorithm for solving the CSSI problem, commonly referred to as the SIDH attack.

**Definition 2 (SIDH diagram).** *Let the following be a commutative diagram consisting of elliptic curves and separable isogenies:*

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi'} \\ E'' & \xrightarrow[\phi']{} & E''' \end{array}$$

*We call the diagram an SIDH diagram if it holds that*

- $\gcd(\deg \phi, \deg \psi) = 1$,
- $\ker \psi' = \phi(\ker \psi)$, *and* $\ker \phi' = \psi(\ker \phi)$.

**Proposition 3 (Kani's lemma [16]).** *Consider the SIDH diagram in Definition 2.*

*Then, there is an isogeny $\Phi$ from $E' \times E'' \to E \times E'''$ represented by*

$$\Phi := \begin{pmatrix} \hat{\phi} & -\hat{\psi} \\ \psi' & \phi' \end{pmatrix}.$$

*Moreover, the kernel of $\Phi$ is given by*

$$\ker \Phi = \langle (\phi(P), -\psi(P)),\ (\phi(Q), -\psi(Q)) \rangle,$$

*where $\{P, Q\}$ is a basis of $E[\deg \phi + \deg \psi]$.*

Robert proved in [22] that Kani's lemma can be extended to principally polarized abelian varieties of higher dimension. In particular, Kani's lemma holds for SIDH diagrams consisting of products of elliptic curves.

Kani's lemma is known to be a powerful tool in isogeny-based cryptography. Indeed, an algorithm derived from Kani's lemma can be used to solve the CSSI problem, which is a variant of the Isogeny problem defined as follows:

**Definition 4 (CSSI problem [15]).** *Let $\mathcal{B}$ be a positive integer, and let $D$ be a positive $\mathcal{B}$-smooth integer (i.e., all prime divisors of $D$ are less than $\mathcal{B}$). Let $E$ and $E'$ be supersingular elliptic curves over $\mathbb{F}_{p^2}$, and let $\{P, Q\}$ and $\{P', Q'\}$ be bases of $E[D]$ and $E'[D]$, respectively. Let $d$ be a positive integer.*

*The* CSSI problem *is the following computational problem:*

*Given $(E, (P, Q), E', (P', Q'), d)$, compute an isogeny $\phi\colon E \to E'$ such that*

$$\phi(P) = P', \qquad \phi(Q) = Q', \qquad \text{and} \qquad \deg \phi = d.$$

Several works [7,19,22] have shown that the CSSI problem can be solved efficiently. More precisely, they exhibit algorithms, called the SIDH attack, that solve the CSSI problem in time polynomial in $\log p$ and $\mathcal{B}$, provided that $d < D^2$.

We next show how the SIDH attack works, especially the most powerful algorithm provided in [22]. The procedure performs as follows:

1. We first compute the integer $c = D^2 - d$, and integers $c_0, c_1, c_2, c_3$ satisfying

$$c = c_0^2 + c_1^2 + c_3^2 + c_4^2,$$

   which can be obtained by Lagrange's four square theorem.
2. Define a matrix $M_c \in M_4(\mathbb{Z})$ by

$$M_c := \begin{pmatrix} c_0 & -c_1 & -c_2 & -c_3 \\ c_1 & c_0 & c_3 & -c_2 \\ c_2 & -c_3 & c_0 & -c_1 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix},$$

   which we denote by $\mathsf{Mat}(c_0, c_1, c_2, c_3)$. We here note that ${}^tM_c \cdot M_c = cI_4$, $M_c \cdot {}^tM_c = cI_4$, and $-M_c = {}^tM_c$.

3. Construct an SIDH diagram as:

$$\begin{array}{ccc} E^4 & \xrightarrow{\phi I_4} & E'^4 \\ {\scriptstyle M_c}\downarrow & & \downarrow{\scriptstyle M_c} \\ E^4 & \xrightarrow[\phi I_4]{} & E'^4 \end{array}$$

4. We have an isogeny $\Phi\colon E'^4 \times E^4 \to E^4 \times E'^4$ and its dual $\hat{\Phi}$ defined by

$$\Phi := \begin{pmatrix} \hat{\phi} I_4 & -{}^tM_c \\ M_c & \phi I_4 \end{pmatrix}, \qquad \text{and} \qquad \hat{\Phi} := \begin{pmatrix} \phi I_4 & {}^tM_c \\ -M_c & \hat{\phi} I_4 \end{pmatrix}.$$

5. We define $G_0$ and $G_1$ by

$$G_0 := \ker \Phi \cap (E'^4 \times E^4)[D], \quad G_1 := \ker \hat{\Phi} \cap (E^4 \times E'^4)[D].$$

6. It follows from Kani's lemma and $c + \deg \phi = D^2$ that

$$G_0 = \langle (P' \cdot \mathbf{v}_i, P \cdot \mathbf{v}_i {}^tM_c), (Q' \cdot \mathbf{v}_i, Q \cdot \mathbf{v}_i {}^tM_c) \rangle_{i=1,2,3,4},$$

$$G_1 = \langle (P \cdot \mathbf{v}_i M_c, -P' \cdot \mathbf{v}_i), (Q \cdot \mathbf{v}_i M_c, -Q' \cdot \mathbf{v}_i) \rangle_{i=1,2,3,4},$$

   where $\mathbf{v}_i$ is the $i$th standard basis vector in $\mathbb{Z}^4$.
7. By using formulas of higher-dimensional isogeny computations (*e.g.,* [18]), we compute two isogenies

$$\Phi_0\colon E'^4 \times E^4 \longrightarrow (E'^4 \times E^4)/G_0,$$
$$\Phi_1\colon E^4 \times E'^4 \longrightarrow (E^4 \times E'^4)/G_1.$$

8. We can prove that $\Phi = \hat{\Phi}_1 \circ \Phi_0$. Therefore, we can compute the isogeny $\Phi$, which contains the solution of the CSSI problem, $\phi$.

### 2.3 POKÉ

In this subsection, we describe POKÉ, an isogeny-based public-key encryption (PKE) scheme proposed in [2]. There are two variants of POKÉ, namely POKÉ-2D and POKÉ-4D. We first present a general construction of POKÉ, and then describe the specific instantiations POKÉ-2D and POKÉ-4D.

*Remark 5.* In the literature, the term "POKÉ" typically refers to POKÉ-2D. However, in this paper, "POKÉ" will be used to denote both POKÉ-2D and POKÉ-4D.

**General construction.** The construction of POKÉ involves the use of SIDH diagrams. However, if one employs SIDH diagrams naively, the scheme can be broken in polynomial time by the SIDH attack. To circumvent this, POKÉ successfully incorporates the SIDH diagrams by employing the following two techniques, which render the setting of the SIDH attack inapplicable:

- concealing the information of $\deg \phi$,
- obscuring the actual images of the torsion points by multiplying them with two distinct scalars.

We now describe the POKÉ protocol in detail.

**Key Generation:** Let $A$, $B$, and $C$ be $\mathcal{B}$-smooth integers that are pairwise coprime. We put $D := BC$. Choose a prime $p$ such that $AD \mid (p+1)$. Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Fix a basis $(R_0, S_0)$ of $E[A]$, a basis $(P, Q)$ of $E[D]$. Draw an integer $d$ uniformly at random from a fixed set $\Delta$, and compute an isogeny $\phi\colon E \to E'$ of degree $d$. Define the torsion points as

$$\begin{aligned} (R_0', S_0') &:= (\alpha\phi(R_0),\, \beta\phi(S_0)), & \alpha, \beta &\in (\mathbb{Z}/A\mathbb{Z})^\times, \\ (P', Q') &:= (\gamma\phi(P),\, \gamma\phi(Q)), & \gamma &\in (\mathbb{Z}/D\mathbb{Z})^\times. \end{aligned}$$

The public key is defined as

$$\mathbf{pk} := (E, (P, Q), (R_0, S_0), E', (P', Q'), (R_0', S_0')),$$

and the secret key as

$$\mathbf{sk} := (d, \alpha, \beta).$$

**Encryption:** Pick a random scalar $s \in (\mathbb{Z}/B\mathbb{Z})^\times$ and compute the two isogenies

$$\begin{aligned} \psi\colon E \to E'' &:= E/\langle C(P + sQ)\rangle, \\ \psi'\colon E' \to E''' &:= E'/\langle C(P' + sQ')\rangle. \end{aligned}$$

Define the auxiliary torsion points by

$$\begin{aligned} (R, S) &:= (\omega\,\psi(R_0),\, \omega^{-1}\psi(S_0)), \\ (R', S') &:= (\omega\,\psi'(R_0'),\, \omega^{-1}\psi'(S_0')), \\ (P_C, Q_C) &:= (B\psi(P), B\psi(Q)) \cdot \mathbf{C}, \\ (P_C', Q_C') &:= (B\psi'(P'), B\psi'(Q')) \cdot \mathbf{C}, \end{aligned}$$

where $\omega$ is a random element of $(\mathbb{Z}/A\mathbb{Z})^\times$ and $\mathbf{C} \in \mathrm{SL}_2(\mathbb{Z}/C\mathbb{Z})$ is sampled uniformly at random. Given a plaintext $\mu$, compute

$$\xi := \mu \oplus \mathrm{KDF}(P_C', Q_C'),$$

where $\oplus$ denotes bitwise XOR and KDF is a key-derivation function. The ciphertext is

$$\mathbf{ct} := ((E'', (P_C, Q_C), (R, S)), (E''', (R', S')), \xi).$$

**Decryption:** Using the secret scalars $(\alpha, \beta)$, compute

$$R'_1 := \alpha^{-1} R', \qquad S'_1 := \beta^{-1} S'.$$

Next, compute an isogeny

$$\phi' \colon E'' \to E'''$$

of degree $d$ by adapting the SIDH attack to the instance

$$(E'', (R, S), E''', (R', S')).$$

Finally, recover the plaintext as

$$\mu' := c \oplus \mathrm{KDF}\big(\phi'(P_C), \phi'(Q_C)\big).$$

The essential component of the POKÉ protocol is the construction of the following SIDH diagram. By employing several additional techniques, we ensure that only a party possessing the isogeny $\phi$ is able to compute the bottom isogeny $\phi'$, which derives a key to recover the plaintext.

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi'} \\ E'' & \xrightarrow[\phi']{} & E''' \end{array}$$

**Parameter choices for POKÉ-2D.** The difference between POKÉ-2D and POKÉ-4D arises in the decryption procedure. In the POKÉ-2D setting, the SIDH attack can be carried out using a 2-dimensional isogeny, which results in a relatively efficient decryption algorithm.

To realize the 2-dimensional SIDH attack, we define the set $\Delta$ by

$$\Delta := \{q(A - q) \mid q \in \{1, \ldots, A - 1\}\}.$$

The remaining parameters are chosen as

$$A \approx 2^{\lambda}, \qquad B \approx 2^{2\lambda}, \qquad C \approx 2^{\lambda/3},$$

where $\lambda$ denotes the security parameter.

POKÉ-2D instantiated with the above parameter choices is conjectured to achieve $\lambda$-bit security.

**Parameter choices for POKÉ-4D.** In the POKÉ-4D setting, the decryption procedure requires the use of a 4-dimensional isogeny, whose computation is less efficient than that of a 2-dimensional isogeny (*e.g.,* see [8]). Consequently, POKÉ-4D incurs a loss in decryption efficiency. On the other hand, it achieves more compact parameters and a more efficient encryption algorithm.

In contrast to POKÉ-2D, we define the set $\Delta$ by

$$\Delta := \left\{ A^2 - q_1^2 - q_2^2 \;\middle|\; 0 < q_1^2 + q_2^2 < A^2,\ q_1, q_2 \in \mathbb{Z} \right\}.$$

The remaining parameters are chosen as

$$A \approx 2^{\lambda/2}, \qquad B \approx 2^{2\lambda}, \qquad C \approx 2^{\lambda/3},$$

where $\lambda$ denotes the security parameter.

According to the security analysis in the original POKÉ paper [2], the above parameter choices are intended to provide $\lambda$-bit security for POKÉ-4D.

## 3 Weak keys of POKÉ with polynomial-time attacks

In this section, we show that certain public keys in POKÉ admit a polynomial-time attack. At the same time, we demonstrate that the existence of such public keys does not compromise the security of POKÉ-2D, because the probability that a public key of this form is sampled is approximately $2^{-\lambda}$, where $\lambda$ denotes the security parameter. By contrast, in the context of POKÉ-4D, this class of weak keys may pose a security risk, since the corresponding sampling probability is larger than $2^{-\lambda}$.

### 3.1 Target problem

We begin by formally defining our target problem, which is closely related to the security of POKÉ. Once the problem has been defined, we focus exclusively on its solutions.

**Definition 6 (Masked-degree Isogeny problem with torsions).** *Let $p$ be a prime, and let $A$ and $D$ be positive integers such that $A|(p+1)$ and $D|(p+1)$. Let $E$ and $E'$ be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\{P, Q\}$ be a basis of $E[D]$, and let $\{P', Q'\}$ be a basis of $E'[D]$. Let $\Delta$ be a set of positive integers.*

*The Masked-degree Isogeny problem with torsions is stated as:*

*From $(E, (P, Q), E', (P', Q'), \Delta)$, compute an isogeny $\phi$ such that*

$$\deg \phi \in \Delta, \quad P' = \gamma\phi(P), \quad \text{and} \quad Q' = \gamma\phi(Q),$$

*where $\gamma \in (\mathbb{Z}/D\mathbb{Z})^\times$.*

It is trivial that, if there is an algorithm that solves the Masked-degree Isogeny problem with torsions with parameters of POKÉ, then there is an algorithm that can break POKÉ.

From now on, we focus on the problem with the following parameters, which come from actual POKÉ's parameters:

- $\lambda$: the security parameter,
- $\mathcal{B}$: a positive integer,

- $A$: a $\mathcal{B}$-smooth integer with $\log_2 A = \mathrm{poly}(\lambda)$,
- $t$: a positive integer,
- $D$: a $\mathcal{B}$-smooth integer such that $\log_2 D = \mathrm{poly}(\lambda)$, $D > A$, $\gcd(A, D) = 1$, and the number of prime factors of $D$ is bounded by $t$,
- $p$: a prime with $p \approx AD$ and $AD|(p+1)$,
- $\Delta := \{q(A-q) \mid q \in \{1, \ldots, A-1\}\}$ for POKÉ-2D, and $\Delta := \{A^2 - q_1^2 - q_2^2 \mid 0 < q_1^2 + q_2^2 < A^2\}$ for POKÉ-4D,
- $\delta_{\mathsf{m}} := \max \Delta$.

### 3.2 Polynomial-time attack on POKÉ with specific public keys

In this subsection, we demonstrate that the Masked-degree Isogeny problem with torsions can be solved in polynomial time for certain parameter choices. This implies that POKÉ admits a polynomial-time break when instantiated with specific public key structures.

**Theorem 7.** *Let $D'$ be a positive integer with $D' \geq \sqrt{\delta_{\mathsf{m}}}$ and $D' \mid D$. If there is an isogeny $\phi$, which is a solution of the Masked-degree Isogeny problem with torsions, such that there is an integer $c$ satisfying*

$$D'^2 - \deg \phi = c^2,$$

*then there is an algorithm that computes $\phi$ in time polynomial in $\mathcal{B}$, $2^t$, and $\lambda$.*

*Proof.* We define an integer $d$ by $d := D/D'$, and set

$$(P_0, Q_0) := (dP, dQ), \qquad (P_0', Q_0') := (dP', dQ').$$

Then $(P_0, Q_0)$ and $(P_0', Q_0')$ form bases of $E[D']$ and $E'[D']$, respectively.

Let $N \in \mathbb{Z}/D'\mathbb{Z}$ be an element satisfying

$$\gamma^2 \deg \phi \equiv N \pmod{D'},$$

which can be computed from $(P_0, Q_0)$, $(P_0', Q_0')$, and the Weil pairing. We consider the quadratic equation

$$x^2 + N = 0$$

in $\mathbb{Z}/D'\mathbb{Z}$. The number of solutions to this equation is bounded by $2^{t+1}$.

Let $x_0 \in \mathbb{Z}/D'\mathbb{Z}$ be such that $x_0 \equiv c\gamma \pmod{D'}$. Clearly, $x_0$ is a solution of $x^2 + N = 0$. Hence, by solving this equation, we obtain a set $X$ with $\#X \leq 2^{t+1}$ and $x_0 \in X$.

We next consider the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle c}\downarrow & & \downarrow{\scriptstyle c} \\ E & \xrightarrow[\phi]{} & E' \end{array}$$

By Kani's lemma, we may define a $D'^2$-isogeny $\Phi\colon E' \times E \to E \times E'$ and its dual $\hat{\Phi}\colon E \times E' \to E' \times E$ by

$$\Phi := \begin{pmatrix} \hat{\phi} & -c \\ c & \phi \end{pmatrix}, \quad \hat{\Phi} := \begin{pmatrix} \phi & c \\ -c & \hat{\phi} \end{pmatrix}.$$

Since $\gamma \in (\mathbb{Z}/D\mathbb{Z})^\times$, we have

$$\begin{aligned} \ker \Phi \cap (E' \times E)[D'] &= \langle (\gamma\phi(P_0), c\gamma P_0), (\gamma\phi(Q_0), c\gamma Q_0) \rangle \\ &= \langle (P'_0, x_0 P_0), (Q'_0, x_0 Q_0) \rangle, \end{aligned}$$

$$\begin{aligned} \ker \hat{\Phi} \cap (E \times E')[D'] &= \langle (c\gamma P_0, -\gamma\phi(P_0)), (c\gamma Q_0, -\gamma\phi(Q_0)) \rangle \\ &= \langle (x_0 P_0, -P'_0), (x_0 Q_0, -Q'_0) \rangle. \end{aligned}$$

Therefore, if $x_0$ is known, we can compute $\Phi$, and hence recover $\phi$, in time polynomial in $\mathcal{B}$ and $\lambda$.

By applying the above procedure to all elements of $X$, we can compute $\phi$ in time polynomial in $\mathcal{B}$, $2^t$, and $\lambda$. This completes the proof of Theorem 7. □

Algorithm 1 demonstrates the algorithm appearing in the proof of Theorem 7.

**Algorithm 1** Attacking POKÉ when $D'^2 - \deg\phi = c^2$

**Require:** $(E, (P, Q))$, $(E', (P', Q'))$, and $D'$
**Ensure:** An isogeny $\phi\colon E \to E'$ such that there is $\gamma \in (\mathbb{Z}/D\mathbb{Z})^\times$ satisfying $Q' = \gamma\phi(P)$ and $Q' = \gamma\phi(Q)$

$d \leftarrow D/D'$
$(P_0, Q_0) \leftarrow (dP, dQ)$
$(P'_0, Q'_0) \leftarrow (dP', dQ')$
$e_0 \leftarrow e(P_0, Q_0)$, where $e$ is the Weil pairing
$e_1 \leftarrow e(P'_0, Q'_0)$
Compute $N \in (\mathbb{Z}/D'\mathbb{Z})^\times$ such that $e_1 = e_0^N$
$X \leftarrow$ the set of roots of $x^2 + N = 0$
**for all** $x \in X$ **do**
  $G_0 \leftarrow \langle (P'_0, xP_0), (Q'_0, xQ_0) \rangle$
  $G_1 \leftarrow \langle (xP_0, -P'_0), (xQ_0, -Q'_0) \rangle$
  Compute $\Phi_0\colon E' \times E \to V_0 := (E' \times E)/G_0$
  Compute $\Phi_1\colon E' \times E \to V_1 := (E \times E')/G_1$
  **if** $V_0 \cong V_1$ **then**
    $\Phi \leftarrow \hat{\Phi}_1 \circ \Phi_0$
    Define $\phi$ by $\Phi = \begin{pmatrix} * & * \\ * & \phi \end{pmatrix}$
    **return** $\phi$
  **end if**
**end for**
**return** $\perp$

*Remark 8.* We stress that, in Algorithm 1, the integer $c$ itself is not required. Rather, it suffices to know $c\gamma \bmod D'$ in order to solve the problem.

*Remark 9.* In the actual POKÉ setting, we have $\mathcal{B} \leq 5$ and $t \leq 2$. Consequently, both $\mathcal{B}$ and $2^t$ are small and do not significantly affect the complexity of Algorithm 1.

*Remark 10.* LIT-SiGamal [20], an isogeny-based PKE scheme, exhibits a structural similarity to POKÉ. In the LIT-SiGamal setting, one employs a secret isogeny whose degree is determined by subtracting a fixed constant from a square of an integer.

One might therefore conjecture that LIT-SiGamal is vulnerable to Algorithm 1. However, Algorithm 1 cannot be directly adapted to LIT-SiGamal, since the orders of the given torsion subgroups are relatively small compared to $\deg \phi$, making it infeasible to select suitable pairs $(P_0, Q_0)$ and $(P'_0, Q'_0)$.

Theorem 7 may provide insight into the security of POKÉ; however, it applies only to very restricted cases. For this reason, we introduce the following generalization of Theorem 7.

**Theorem 11.** *Let $D'$ be a positive integer with $D' \geq \sqrt{\delta_{\mathsf{m}}}$ and $D' \mid D$. We fix an integer $r$. If there is an integer $c$ such that*

$$D'^2 - \deg \phi = r \cdot c^2,$$

*then there is an algorithm that solves the Masked-degree Isogeny problem with torsions in time polynomial in $\mathcal{B}$, $2^t$, and $\lambda$.*

*Proof.* We define $(P_0, Q_0)$, $(P'_0, Q'_0)$, and $N$ by the same way as in the proof of Theorem 7. We consider the quadratic equation in $\mathbb{Z}/D'\mathbb{Z}$

$$r \cdot x^2 + N = 0,$$

which has at most $2^{t+1}$ roots.

We let $x_0$ be an element in $\mathbb{Z}/D'\mathbb{Z}$ such that $x_0 \equiv c\gamma \pmod{D'}$. Then, the element $x_0$ is a root of the equation $r \cdot x^2 + N = 0$. Therefore, solving this equation, we obtain a set $X$ with $\#X \leq 2^{t+1}$ and $x_0 \in X$.

Let $r_0, r_1, r_2, r_3$ be integers satisfying

$$r = r_0^2 + r_1^2 + r_2^2 + r_3^2,$$

and let $M_r$ be a $4 \times 4$-matrix given by

$$M_r := \mathsf{Mat}(r_0, r_1, r_2, r_3).$$

We consider the commutative diagram

$$\begin{array}{ccc} E^4 & \xrightarrow{\phi I_4} & E'^4 \\ {\scriptstyle cM_r}\downarrow & & \downarrow{\scriptstyle cM_r} \\ E^4 & \xrightarrow[\phi I_4]{} & E'^4 \end{array}$$

By Kani's lemma, we may define a $D'^2$-isogeny $\Phi\colon E'^4 \times E^4 \to E^4 \times E'^4$ and its dual $\hat{\Phi}$ by

$$\Phi := \begin{pmatrix} \hat{\phi} I_4 & -c^t M_r \\ cM_r & \phi I_4 \end{pmatrix}, \quad \hat{\Phi} := \begin{pmatrix} \phi I_4 & c^t M_r \\ -cM_r & \hat{\phi} I_4 \end{pmatrix}.$$

Then we have the following:

$$\begin{aligned} &\ker \Phi \cap (E'^4 \times E^4)[D'] \\ &= \langle (\gamma\phi(P_0) \cdot \mathbf{v}_i, c\gamma P_0 \cdot \mathbf{v}_i {}^t M_r), (\gamma\phi(Q_0) \cdot \mathbf{v}_i, c\gamma Q_0 \cdot \mathbf{v}_i {}^t M_r) \rangle_{i=1,2,3,4} \\ &= \langle (P'_0 \cdot \mathbf{v}_i, x_0 P_0 \cdot \mathbf{v}_i {}^t M_r), (Q'_0 \cdot \mathbf{v}_i, x_0 Q_0 \cdot \mathbf{v}_i {}^t M_r) \rangle_{i=1,2,3,4}, \end{aligned}$$

$$\begin{aligned} &\ker \hat{\Phi} \cap (E^4 \times E'^4)[D'] \\ &= \langle (c\gamma P_0 \cdot \mathbf{v}_i M_r, -\gamma\phi(P_0) \cdot \mathbf{v}_i), (c\gamma Q_0 \cdot \mathbf{v}_i M_r, -\gamma\phi(Q_0) \cdot \mathbf{v}_i) \rangle_{i=1,2,3,4} \\ &= \langle (x_0 P_0 \cdot \mathbf{v}_i M_r, -P'_0 \cdot \mathbf{v}_i), (x_0 Q_0 \cdot \mathbf{v}_i M_r, -Q'_0 \cdot \mathbf{v}_i) \rangle_{i=1,2,3,4}, \end{aligned}$$

where $\mathbf{v}_i$ is the $i$-th standard basis vector in $\mathbb{Z}^4$. Therefore, if $x_0$ is known, we can recover $\phi$ in time polynomial in $\mathcal{B}$ and $\lambda$.

This completes the proof of Theorem 11. □

We summarize the algorithm appearing in the proof of Theorem 11 as Algorithm 2.

Theorem 11 implies that if an adversary can correctly guess the value of $r$, then such an adversary would be capable of breaking POKÉ in polynomial time. Therefore, to analyze the attack from Algorithm 2, we need to estimate the probability that a random public key satisfies the equation

$$D'^2 - \deg \phi = r \cdot c^2$$

for a fixed integer $r$.

### 3.3 Distribution on the weak keys with polynomial-time attacks

To the beginning, we define "weak keys" of POKÉ associated with $D'$ and $r$ based on Theorem 11.

**Definition 12 (Weak keys of POKÉ associated with $D'$ and $r$).** *Let $D'$ be a positive integer with $D' \mid D$, and let $r$ be a square-free integer.*

*Let an isogeny $\phi$ be a solution of the Masked-degree Isogeny problem with torsions. If there is an integer $c$ satisfying*

$$D'^2 - \deg \phi = r \cdot c^2,$$

*then we call $\phi$ a weak key of POKÉ associated with $D'$ and $r$.*

**Algorithm 2** Attacking POKÉ with $D'^2 - \deg\phi = r \cdot c^2$

**Require:** $(E, (P, Q))$, $(E', (P', Q'))$, $D'$, and $r$
**Ensure:** An isogeny $\phi\colon E \to E'$ such that there is $\gamma \in (\mathbb{Z}/D\mathbb{Z})^\times$ satisfying $P' = \gamma\phi(P)$ and $Q' = \gamma\phi(Q)$

$d \leftarrow D/D'$
$(P_0, Q_0) \leftarrow (dP, dQ)$
$(P'_0, Q'_0) \leftarrow (dP', dQ')$
Find integers $r_0, r_1, r_2, r_3$ with $r = r_0^2 + r_1^2 + r_2^2 + r_3^2$
$M_r \leftarrow \mathsf{Mat}(r_0, r_1, r_2, r_3)$
$e_0 \leftarrow e(P_0, Q_0)$
$e_1 \leftarrow e(P'_0, Q'_0)$
Compute $N \in (\mathbb{Z}/D'\mathbb{Z})^\times$ such that $e_1 = e_0^N$
**for all** roots of $r \cdot x^2 + N = 0$ over $\mathbb{Z}/D'\mathbb{Z}$ **do**
  $G_0 \leftarrow \langle (P'_0 \cdot \mathbf{v}_i, xP_0 \cdot \mathbf{v}_i {}^tM_r), (Q'_0 \cdot \mathbf{v}_i, xQ_0 \cdot \mathbf{v}_i {}^tM_r) \rangle_{i=1,2,3,4}$
  $G_1 \leftarrow \langle (xP_0 \cdot \mathbf{v}_i M_r, -P'_0 \cdot \mathbf{v}_i), (xQ_0 \cdot \mathbf{v}_i M_r, -Q'_0 \cdot \mathbf{v}_i) \rangle_{i=1,2,3,4}$
  Compute $\Phi_0\colon E'^4 \times E^4 \to V_0 := (E'^4 \times E^4)/G_0$
  Compute $\Phi_1\colon E^4 \times E'^4 \to V_1 := (E^4 \times E'^4)/G_1$
  **if** $V_0 \cong V_1$ **then**
    $\Phi \leftarrow \hat{\Phi}_1 \circ \Phi_0$
    Define $\phi$ by $\Phi = \begin{pmatrix} * & * \\ * & \phi I_4 \end{pmatrix}$
    **return** $\phi$
  **end if**
**end for**
**return** $\perp$

In this subsection, we study the probability that a randomly chosen public key of POKÉ, *i.e.*, a solution to the Masked-degree Isogeny problem with torsions, becomes a weak key of POKÉ associated with $D'$ and $r$.

To simplify the analysis, especially for both cases of POKÉ-2D and POKÉ-4D, we adopt the following heuristic, which allows us to model the distribution on $D'^2 - \deg\phi$ as a uniform distribution as far as we consider the square-free part of $D'^2 - \deg\phi$.

**Heuristic 1.** Let $r$ be a square-free integer. Then it holds that

$$\begin{aligned}&\Pr[r \text{ is the square-free part of } D'^2 - \delta \mid \delta \in \Delta]\\ \approx\ &\Pr[r \text{ is the square-free part of } D'^2 - \delta_0 \mid \delta_0 \in \{1, \ldots, \delta_{\mathsf{m}}\}].\end{aligned}$$

*Remark 13.* We do not provide a rigorous proof of Heuristic 1. Instead, in Section 5.3, we present experimental results that allow us to compare the theoretical probabilities of the occurrence of weak keys, derived directly from Heuristic 1, with the empirical frequencies observed in our experiments.

The close agreement between the theoretical predictions and the experimental data suggests that Heuristic 1 could capture the underlying distribution.

**Theorem 14.** *Assume that Heuristic 1. For a fixed integer $r$, the probability that Algorithm 2 succeeds for a random public key of POKÉ is approximately*

$$\frac{1}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}} \cdot \frac{1}{\sqrt{r}}.$$

*Proof.* By Heuristic 1, we may assume that $\deg\phi$ is uniformly distributed over $\{1, \ldots, \delta_{\mathsf{m}}\}$. Under this assumption, the probability can be estimated as

$$\begin{aligned}\Pr[\deg\phi = D'^2 - r \cdot c^2] &= \frac{1}{\delta_{\mathsf{m}}} \cdot \#\left\{c \in \mathbb{Z} \mid 0 < D'^2 - r \cdot c^2 < \delta_{\mathsf{m}}\right\}\\ &\approx \frac{1}{\delta_{\mathsf{m}}} \cdot \frac{\sqrt{D'^2} - \sqrt{D'^2 - \delta_{\mathsf{m}}}}{\sqrt{r}}\\ &= \frac{1}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}} \cdot \frac{1}{\sqrt{r}}.\end{aligned}$$

This completes the proof of Theorem 14. □

Theorem 14 immediately implies the following corollary.

**Corollary 15.** *We assume Heuristic 1. The probability that Algorithm 2 succeeds for a random public key of POKÉ is the largest if $D'^2 \approx \delta_{\mathsf{m}}$, and the probability is approximately*

$$\frac{1}{\sqrt{\delta_{\mathsf{m}}}} \cdot \frac{1}{\sqrt{r}}.$$

Since $r$ satisfies $1 \leq r \lesssim \delta_{\mathsf{m}}$, we have

$$\frac{1}{\delta_{\mathsf{m}}} \ \lesssim\ \frac{1}{\sqrt{\delta_{\mathsf{m}}}} \cdot \frac{1}{\sqrt{r}} \ \leq\ \frac{1}{\sqrt{\delta_{\mathsf{m}}}}.$$

In the concrete parameterization of POKÉ-2D, the parameter $\delta_{\mathsf{m}}$ is instantiated to be on the order of $A^2 \approx 2^{2\lambda}$. Consequently, for a square-free integer $r$, the success probability of Algorithm 2 is bounded above by $2^{-\lambda}$, and thus negligible. It follows that Algorithm 2 does not compromise the security of POKÉ-2D.

By contrast, in the POKÉ-4D setting, where we set $\delta_{\mathsf{m}} \approx 2^{\lambda}$, the success probability of Algorithm 2 is approximately $2^{-\lambda+\epsilon/2}$ when $r = 2^{\lambda-\epsilon}$ for some $\epsilon \in [0, \lambda]$. For almost all choices of $\epsilon$, this probability exceeds $2^{-\lambda}$, and hence it gives rise to a security concern for POKÉ-4D.

Table 1 summarizes the arguments in this section on weak keys of POKÉ-2D and POKÉ-4D.

**Table 1.** Weak keys of POKÉ

| | POKÉ-2D | POKÉ-4D |
|---|---|---|
| Attack | polynomial-time | polynomial-time |
| Probability of occurrence | less than $1/2^{\lambda}$ | $1/2^{\lambda-\epsilon/2}$ with $\epsilon \in [0, \lambda]$ |

## 4 Weak-key attack on POKÉ

In the previous section, we showed that POKÉ can be broken in polynomial time for certain public keys. The probability of sampling such weak keys is bounded above by $2^{-\lambda}$ in the POKÉ-2D setting, whereas in the POKÉ-4D setting it is bounded below by $2^{-\lambda}$.

In this section, we depart from the pursuit of a polynomial-time attack on POKÉ and instead investigate an attack that applies to a broader class of public keys. This perspective could enable a more comprehensive analysis of the security of POKÉ.

### 4.1 Attack on POKÉ with weak keys

We present a generalization of the attack described in Theorem 11, which enables the use of a larger set of "weak keys" at the cost of increased attack complexity.

Specifically, the following procedure outlines our attack:

1. An adversary fixes a set $\mathcal{R} \subset \{1, \ldots, \delta_{\mathsf{m}}\}$ consisting of square-free integers.
2. The adversary runs Algorithm 2 for each $r \in \mathcal{R}$.

Algorithm 3 presents the proposed attack.

**Definition 16 (Weak keys of POKÉ associated with $\mathcal{R}$).** *Let $\mathcal{R}$ be a set of square-free integers with $\mathcal{R} \subset \{1, \ldots, \delta_{\mathsf{m}}\}$.*

**Algorithm 3** Attacking POKÉ with weak keys

**Require:** $(E,(P,Q))$, $(E',(P',Q'))$, $D'$, and $\mathcal{R}$
**Ensure:** An isogeny $\phi\colon E \to E'$ such that there is $\gamma \in (\mathbb{Z}/D\mathbb{Z})^\times$ satisfying $P' = \gamma\phi(P)$ and $Q' = \gamma\phi(Q)$

```
for all r ∈ R do
    Compute φ from Algorithm 2 using (E,(P,Q)), (E',(P',Q')), D', and r
    if φ ≠ ⊥ then
        return φ
    end if
end for
return ⊥
```

*Let $\phi$ be an isogeny that solves the Masked-degree Isogeny Problem with torsions. If there exist integers $c$ and $r \in \mathcal{R}$ such that*

$$D'^2 - \deg\phi = rc^2,$$

*then we call $\phi$ a weak key of POKÉ associated with $\mathcal{R}$, or simply an $\mathcal{R}$-weak key.*

**Theorem 17.** *Under Heuristic 1, a random solution of the Masked-degree Isogeny problem with torsions becomes a weak key of POKÉ associated with $\mathcal{R}$ and $D'$ with probability*

$$\frac{1}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}} \sum_{r\in\mathcal{R}} \frac{1}{\sqrt{r}}.$$

*In particular, if $D'^2 \approx \delta_{\mathsf{m}}$, then the probability is*

$$\frac{1}{\sqrt{\delta_{\mathsf{m}}}} \sum_{r\in\mathcal{R}} \frac{1}{\sqrt{r}}.$$

*Moreover, if a solution of the Masked-degree Isogeny problem with torsions is an $\mathcal{R}$-weak key, then the problem can be solved in*

$$O(\#\mathcal{R} \cdot \mathrm{poly}(\mathcal{B}, 2^t, \lambda)).$$

*Proof.* The assertion immediately follows from Theorems 11 and 14. □

Consequently, a random public key of POKÉ admits an attack in time $\tilde{O}(\#\mathcal{R})$ with probability

$$\frac{1}{\sqrt{\delta_{\mathsf{m}}}} \sum_{r\in\mathcal{R}} r^{-1/2}.$$

These quantities depend intimately on the choice of $\mathcal{R}$. Thus, in the following subsection, we discuss a choice of the set $\mathcal{R}$ that optimizes this trade-off, and we describe the resulting complexity and probability of occurrence of weak keys.

### 4.2 Attack from the optimized $\mathcal{R}$

The optimized choice of $\mathcal{R}$ attains the maximum probability of occurrence of weak keys of POKÉ for a fixed value of $\#\mathcal{R}$. Therefore, the desired set $\mathcal{R}$ comprises the smallest $\#\mathcal{R}$ square-free integers.

Let $n$ denote the cardinality of $\mathcal{R}$. We estimate the probability of occurrence of a weak key of POKÉ associated with $\mathcal{R}$, where $\mathcal{R}$ consists of the $n$ smallest square-free integers.

To begin, we prove the following lemma.

**Lemma 18.** *Let $n$ be a positive integer, and we denote by $s_i$, the $i$th positive square-free integer.*

*Then, it holds that*

$$\sum_{i=1}^{n} \frac{1}{\sqrt{s_i}} = \frac{2\sqrt{6}}{\pi}\sqrt{n} + O(\log n).$$

*Proof.* Let $x$ be a positive real number, and let

$$\mathrm{Sq}\colon \mathbb{R}_{>0} \to \mathbb{Z}$$

denote the function that returns the number of positive square-free integers in the interval $[0, x]$. Then, it follows from [13, Theorem 333] that

$$\mathrm{Sq}(x) = \frac{6}{\pi^2}x + O(\sqrt{x}),$$

whence we have

$$s_i = \frac{\pi^2}{6}i + O(\sqrt{i}).$$

From the above evaluation, it is easy to see that

$$\frac{1}{\sqrt{s_i}} = \frac{\sqrt{6}}{\pi} \cdot \frac{1}{\sqrt{i}} + O(i^{-1}).$$

Therefore, it follows from the Euler–Maclaurin formula that

$$\begin{aligned}\sum_{i=1}^{n} \frac{1}{\sqrt{s_i}} &= \frac{\sqrt{6}}{\pi}\int_1^n \frac{1}{\sqrt{x}}\,dx + O(1) + \sum_{i=1}^{n} O(i^{-1}) \\ &= \frac{2\sqrt{6}}{\pi}\sqrt{n} + O(\log n).\end{aligned}$$

This completes the proof of the assertion. □

**Theorem 19.** *We let $\mathcal{R}$ be a set*

$$\mathcal{R} = \{s_1, \ldots, s_n\}.$$

*Then, the complexity of Algorithm 3 is $\tilde{O}(n)$ and a random public key of POKÉ becomes a weak key of POKÉ associated with $\mathcal{R}$ and $D'$ with probability approximately*

$$\frac{2\sqrt{6}/\pi}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}}\sqrt{n} = O\left(\frac{\sqrt{n}}{D'}\right).$$

*In particular, if $D'^2 \approx \delta_{\mathsf{m}}$, then the probability is*

$$O\left(\sqrt{\frac{n}{\delta_{\mathsf{m}}}}\right).$$

*Proof.* It follows directly from Theorem 17 and Lemma 18. □

We first consider POKÉ-2D, where the parameter $\delta_{\mathsf{m}}$ satisfies $\delta_{\mathsf{m}} \approx 2^{2\lambda}$. By Theorem 19, POKÉ-2D achieves $(n, \sqrt{n} \cdot 2^{-\lambda})$-security, meaning that any adversary running in time at most $n$ succeeds in breaking the scheme with probability at most $\sqrt{n} \cdot 2^{-\lambda}$. Since

$$n \cdot \left(\frac{\sqrt{n}}{2^{\lambda}}\right)^{-1} = \sqrt{n} \cdot 2^{\lambda},$$

we conclude that POKÉ-2D still achieves $\lambda$-bit security under our novel attack.

In the case of POKÉ-4D, the situation is slightly different. Since $\delta_{\mathsf{m}}$ is approximately $2^{\lambda}$ in this setting, POKÉ-4D achieves $(n, \sqrt{n} \cdot 2^{-\lambda/2})$-security. Consequently, when $n$ is smaller than $2^{\lambda}$, POKÉ-4D may fail to achieve $\lambda$-bit security.

To address this issue, we propose to fix the parameters of POKÉ-4D. Our suggested parameter choices are given in Section 5.

*Remark 20.* Snake Mackerel is an isogeny-based authenticated key encapsulation mechanism proposed in [14]. Since Snake Mackerel employs POKÉ-4D as its KEM component, its parameters must also be modified as in Section 5.

*Remark 21.* INKE is a variant of POKÉ introduced in [17] whose security is also reduced to the hardness of the Masked-degree Isogeny problem with torsions.

In the INKE setting, one sets $A \approx 2^{\lambda}$ and

$$\Delta = \{1, \ldots, A-1\},$$

which implies $\delta_{\mathsf{m}} \approx 2^{\lambda}$. Consequently, since it also holds that $\delta_{\mathsf{m}} \approx 2^{\lambda}$ in the POKÉ-4D instantiation, the induced distribution of weak keys appearing in INKE coincides with that of POKÉ-4D. It follows that the security analysis for POKÉ-4D carries over to INKE, thereby also necessitating an appropriate adjustment of the underlying parameters for INKE (see Remark 24).

**Generation of $\mathcal{R}$.** It may be not a priori obvious how to generate the set $\mathcal{R}$ consisting of the smallest $n$ square-free integers. In this section, we recall a classical method to construct $\mathcal{R}$ in $O(n)$ time.

Our approach is based on a sieving technique. We begin by defining the initial set

$$\mathcal{R}_0 := \{1, 2, \ldots, 2n\}.$$

From $\mathcal{R}_0$, we remove all integers that are divisible by $i^2$ for integers

$$i = 2, \ldots, \left\lfloor \sqrt{2n} \right\rfloor.$$

We then define $\mathcal{R}$ to be the subset of $\mathcal{R}_0$ consisting of its first $n$ remaining elements.

Algorithm 4 describes the above procedure for constructing $\mathcal{R}$. As can be seen from Algorithm 4, the computational complexity of this procedure is

$$O\left(\sum_{i=2}^{\lfloor\sqrt{2n}\rfloor} \left\lfloor \frac{2n}{i^2} \right\rfloor\right) = O(n).$$

Therefore, the generation of $\mathcal{R}$ does not contribute to the overall complexity of the weak-key attack.

**Algorithm 4** Construction of $\mathcal{R}$

**Require:** A positive integer $n$
**Ensure:** The set $\mathcal{R}$ consisting of the smallest $n$ square-free integers
$\mathcal{R}_0 \leftarrow \{1, \ldots, 2n\}$
**for all** $i \in \{2, \ldots \lfloor\sqrt{2n}\rfloor\}$ **do**
  **for all** $j \in \{1, \ldots, \lfloor 2n/i^2 \rfloor\}$ **do**
    $\mathcal{R}_0 \leftarrow \mathcal{R}_0 \setminus \{j \cdot i^2\}$
  **end for**
**end for**
**if** $\#\mathcal{R}_0 < n$ **then**
  **return** $\perp$
**end if**
$\mathcal{R} \leftarrow$ The set consisting of the first $n$ elements in $\mathcal{R}_0$
**return** $\mathcal{R}$

## 5 Countermeasures against the weak-key attack

In this section, we discuss countermeasures against our weak-key attack on POKÉ-4D so that it achieves $\lambda$-bit security.

We first introduce a weak-key-rejection procedure that prevents the generation of weak keys during the key-generation process. However, the effect of this rejection procedure is limited in our setting; consequently, it is also necessary to revise the parameters of POKÉ-4D.

We propose fixed parameters for POKÉ-4D that are resistant to the weak-key attack in Section 4. More precisely, we introduce novel parameter choices for

POKÉ-4D such that, for any $\mathcal{R}$ with $\#\mathcal{R} < 2^\lambda$, the probability that a weak key associated with $\mathcal{R}$ occurs is bounded by $O(\#\mathcal{R}/2^\lambda)$.

We also present experimental results on the probability that a random public key of POKÉ-4D becomes an $\mathcal{R}$-weak key. These experiments demonstrate that our proposed parameters successfully resist the weak-key attack.

### 5.1 Weak-key-rejection process

One possible countermeasure against our weak-key attack is to incorporate a weak-key-rejection process into the key-generation procedure so that weak keys are discarded in advance. However, this approach does not seem to be effective due to the cost of the rejection procedure; namely, the procedure does not improve the security level significantly. We explain the reason below.

Let $m$ be a positive integer, and let $\mathcal{R}'$ be a set of $m$ square-free integers. We now consider a way to generate a public key of POKÉ-4D that is not an $\mathcal{R}'$-weak key.

By Theorem 14, the optimal choice of $\mathcal{R}'$ for rejecting the largest possible number of weak keys is

$$\mathcal{R}' := \{s_1, \ldots, s_m\}.$$

From now on, we fix the set $\mathcal{R}'$ as the above.

Let $n > m$ be positive integers, and define

$$\mathcal{R} := \{s_1, \ldots, s_n\}.$$

By Theorem 19, after excluding all $\mathcal{R}'$-weak keys, the probability that a uniformly random public key remains $\mathcal{R}$-weak is approximately given by

$$\frac{\sqrt{n} - \sqrt{m}}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}}.$$

Furthermore, since the adversary only exploits the subset $\mathcal{R} \setminus \mathcal{R}'$, the computational complexity of the attack is reduced to $\tilde{O}(n - m)$. Consequently, the $\mathcal{R}'$-weak-key rejection process increases the time-success ratio of the attack to

$$\frac{n - m}{\frac{\sqrt{n} - \sqrt{m}}{D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}}} = (\sqrt{n} + \sqrt{m})\big(D' + \sqrt{D'^2 - \delta_{\mathsf{m}}}\big).$$

However, to the best of our knowledge, designing an effective algorithm for rejecting $\mathcal{R}'$-weak keys appears to be difficult. There are two major obstacles to constructing such a rejection procedure:

- detecting $\mathcal{R}'$-weakness of a random public key, and
- generating non-$\mathcal{R}'$-weak keys associated with multiple choices of $D'$.

First, we argue that determining whether a randomly chosen public key is a weak key associated with $\mathcal{R}'$ and $D'$ is computationally infeasible. Indeed, on classical computers, deciding whether a given integer is square-free is believed to

require subexponential time (see, for example, [6] for the currently best-known algorithms). Thus, computing the square-free part of an integer is also computationally hard. Therefore, given a random public key $\phi$, one cannot efficiently recover the square-free integer $r$ satisfying

$$D'^2 - \deg \phi = r \cdot c^2.$$

To address the above issue, one may instead consider a restricted setting in which determining whether $N := D'^2 - \deg \phi$ is square-free becomes tractable. More precisely, rather than computing the square-free part of $N$, we test whether $N$ admits a decomposition of the form

$$N = \prod_{i=1}^{t_\lambda} p_i^{e_i} \times q,$$

where $t_\lambda$ is a positive integer satisfying $t_\lambda = \mathrm{poly}(\lambda)$, $p_i$ denotes the $i$-th prime number, $q$ is a prime satisfying $q > p_{t_\lambda}$, and each exponent $e_i \in \{0, 1\}$. In particular, this condition implies that $N$ is square-free. Furthermore, there exists a polynomial-time algorithm for determining whether $N$ has the above form (see Algorithm 5).

**Algorithm 5** Square-free $N$

**Require:** $N$ and $t_\lambda$
**Ensure:** Determining whether $N$ can be written as $N = \prod_{i=1}^{t_\lambda} p_i^{e_i} \times q$
1: Compute $p' := p_1 \cdots p_{t_\lambda}$
2: $N' \leftarrow N / \gcd(N, p')$
3: **if** $N'$ is prime and $N' > p_\lambda$ **then**
4: **return** TRUE
5: **else**
6: **return** FALSE
7: **end if**

However, the second obstacle prevents effective weak-key rejection. Since the adversary may choose from multiple candidates for $D'$, the adversary can select a value of $D'$ different from those considered in the weak-key-rejection procedure. Consequently, the procedure must ensure that the resulting public key is not an $\mathcal{R}'$-weak key with respect to any $D'$ that could potentially be chosen by the adversary.

Let $u_\lambda$ be a positive integer, and let $D'_1, \ldots, D'_{u_\lambda}$ be candidates for $D'$. We consider a procedure in which the user attempts to avoid $\mathcal{R}'$-weak keys associated with all of $D'_1, \ldots, D'_{u_\lambda}$. The following algorithm generates a desired public key:

1. Generate a random public key $\phi$.
2. For each $i = 1, \ldots, u_\lambda$, check whether

$$N_i := D'^2_i - \deg \phi$$

satisfies the desired property using Algorithm 5.

3. If Algorithm 5 outputs FALSE for some $i$, then return to Step 1.
4. Check whether $N_1, \ldots, N_{u_\lambda}$ belong to $\mathcal{R}'$.
5. If $N_i \in \mathcal{R}'$ for some $i$, then return to Step 1.
6. Output $\phi$.

Since the probability that $N$ is square-free is approximately $6/\pi^2$, the above procedure requires at least

$$\left(\frac{\pi^2}{6}\right)^{u_\lambda} \cdot \mathrm{poly}(\lambda)$$

operations. Thus, in order for the key-generation procedure to run in polynomial time, it is necessary to choose $u_\lambda = O(\log \lambda)$.

Therefore, even when the weak-key-rejection process is taken into account, the adversary can still choose $D'$ satisfying

$$D'^2 \approx \delta_{\mathsf{m}} \cdot \mathrm{poly}(\lambda).$$

Recall that from Theorem 19, POKÉ-4D achieves $(1, 1/D')$-security. Consequently, the security level of POKÉ-4D increases only from $\sqrt{\delta_{\mathsf{m}}}$ to

$$\sqrt{\delta_{\mathsf{m}}} \cdot \mathrm{poly}(\lambda).$$

Hence, the impact of the weak-key-rejection procedure on the overall security is limited.

*Remark 22.* In a practical setting, one might expect that the additional factor "poly($\lambda$)" improves the security level of POKÉ-4D. However, in the POKÉ-4D setting, the adversary can in fact select $D'$ such that $D'^2 \approx \delta_{\mathsf{m}}$. This stems from the structure of $D$, which has exactly two prime factors, namely 3 and 5, and there exist $\Theta(\lambda)$ candidates of $D'$ satisfying $D'^2 \approx \delta_{\mathsf{m}}$.

On the other hand, in the INKE setting, the same additional term can genuinely increase the security level. This is because in the INKE setting, the parameter $D$ is restricted to a prime power of 3, which significantly limits the structure of admissible $D'$ and prevents the adversary from freely choosing values that satisfy $D'^2 \approx \delta_{\mathsf{m}}$.

### 5.2 Suggested parameters of POKÉ-4D

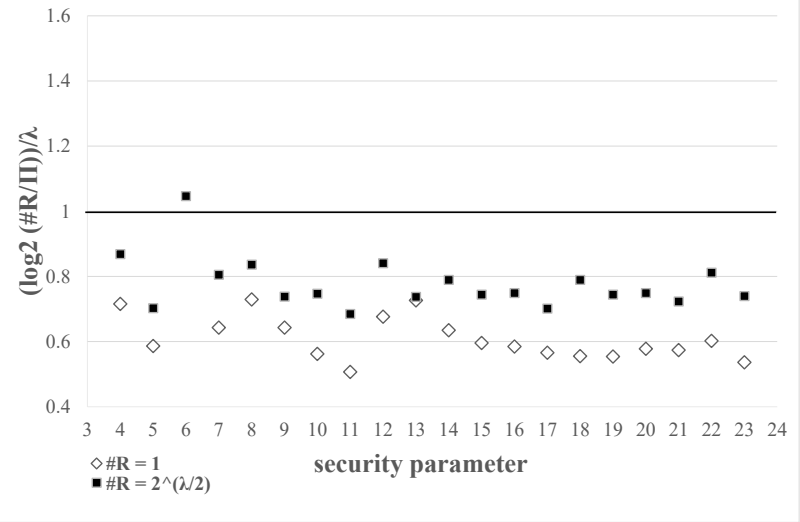
By Theorem 19, the relevant parameters satisfy the relation $\sqrt{n \cdot \delta_{\mathsf{m}}} \approx 2^\lambda$ for all $n \in \{1, \ldots, 2^\lambda\}$. Hence, rather than choosing $\delta_{\mathsf{m}} \approx 2^\lambda$, we set $\delta_{\mathsf{m}} \approx 2^{2\lambda}$; and thus, we have

$$A \approx 2^\lambda.$$

The remaining parameters do not influence the attack described in Theorem 19. Consequently, it suffices to modify only the size of $A$.

The requirement on the suggested parameters for POKÉ-4D is the same as that for POKÉ-2D. Therefore, one can adopt the same parameter choices for POKÉ-4D as those used in POKÉ-2D. Unfortunately, this means that the primary advantage of POKÉ-4D—namely, that it is more compact and admits a more efficient encryption procedure than POKÉ-2D—no longer exists.

**Fig. 1.** Security levels of POKÉ-4D with original parameters




*Remark 23.* From the viewpoint of performance, POKÉ-4D no longer offers an advantage; however, several benefits still remain. For example, the underlying security assumption of POKÉ-4D is conceptually simpler and cleaner than that of POKÉ-2D.

*Remark 24.* As noted in Remark 21, our weak-key attack extends to INKE as well, and consequently the choice of parameters for INKE must be revised.

In the INKE setting, instead of selecting $A \approx 2^{\lambda}$, we set

$$A \approx 2^{2\lambda},$$

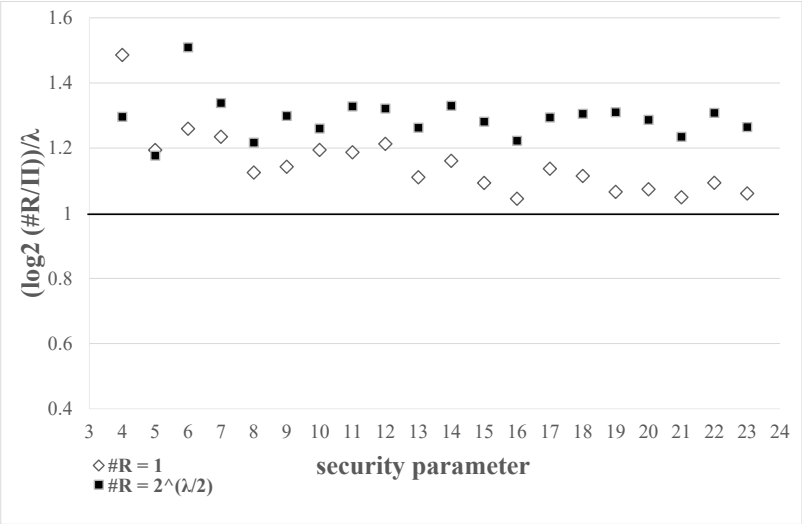
on account of the fact that the probability of a weak-key occurrence in INKE is $O\left(\sqrt{\#\mathcal{R}/\delta_{\mathsf{m}}}\right) = O\left(\sqrt{\#\mathcal{R}/A}\right)$.

If the weak-key-rejection procedure described in Section 5.1 is employed, the parameter sizes can be reduced as discussed in Remark 22. The effectiveness of the weak-key rejection depends on the extent to which an increase in key-generation cost can be tolerated.

### 5.3 Experimentation

In this subsection, we present our experimental results on the security levels of POKÉ-4D for small $\lambda$'s. In particular, we demonstrate that the suggested parameters are resistant to the weak-key attack.

**Fig. 2.** Security levels of POKÉ-4D with suggested parameters




We consider the following four instances of the weak-key attack:

- employing a set $\mathcal{R}$ with $\#\mathcal{R} = 1$ under the original POKÉ-4D parameters;
- employing a set $\mathcal{R}$ with $\#\mathcal{R} \approx 2^{\lambda/2}$ under the original POKÉ-4D parameters;
- employing a set $\mathcal{R}$ with $\#\mathcal{R} = 1$ under the suggested parameters; and
- employing a set $\mathcal{R}$ with $\#\mathcal{R} \approx 2^{\lambda/2}$ under the suggested parameters.

For our experimentation, we defined $A$, $D'$, and $\mathcal{R}$ as follows:

- $A = 2^{\lambda/2}$ for the original POKÉ-4D parameters, and $A = 2^{\lambda}$ for the suggested parameters;
- $D' = 3^{\lfloor \log_3 A \rfloor}$; and
- $\mathcal{R}$ is the set of the smallest $\#\mathcal{R}$ positive square-free integers.

We sampled $q_0$ and $q_1$ uniformly at random from the set $\{1, \ldots, A-1\}$ and tested whether $q_0^2 + q_1^2$ corresponds to a weak key, *i.e.,* whether there exist an integer $c$ and an element $r \in \mathcal{R}$ such that

$$D'^2 - (A^2 - (q_0^2 + q_1^2)) = r \cdot c^2.$$

Let $\Pi_0$ be the theoretical probability of occurrence of weak keys provided in Theorem 19, *i.e.,* $\Pi_0 = \sqrt{\#\mathcal{R}}/A$. By repeating this test $\lfloor 100/\Pi_0 \rfloor$ times, we experimentally estimated the probability of weak-key occurrences in POKÉ-4D for each security parameter $\lambda = 4, \ldots, 23$.

Our experimental results are summarized in Figures 1 and 2. Figure 1 presents the outcomes for the original parameters, while Figure 2 shows the results for the proposed parameters.

We denote by $\Pi$ the experimentally observed probability of weak-key occurrences. We note that POKÉ-4D achieves the $\log_2(\#\mathcal{R}/\Pi)$-bit security. The vertical axes of those figures represent the quantity

$$\frac{\log_2(\#\mathcal{R}/\Pi)}{\lambda}.$$

In particular, the dots above the thick line labeled 1 indicate that POKÉ-4D achieves $\lambda$-bit security. The horizontal axes correspond to the security parameter $\lambda$.

*Remark 25.* If $\Pi = 0$ in our experiments, we omit the corresponding markers from the figures.

As illustrated in Figure 1, the values $\#\mathcal{R}/\Pi$ are, in most cases, smaller than $2^\lambda$. This indicates that the original parameter set of POKÉ-4D does not achieve $\lambda$-bit security. In particular, our experiments show that $\#\mathcal{R}/\Pi \approx 2^{0.78\lambda}$ when the adversary chooses a set $\mathcal{R}$ satisfying $\#\mathcal{R} = 2^{\lambda/2}$. These observations experimentally suggest that, under the original parameters, a randomly chosen public key in POKÉ-4D is susceptible to an attack with complexity $\tilde{O}(2^{\lambda/2})$ with probability approximately $2^{-0.28\lambda}$, which is close to the theoretical probability $2^{-\lambda/4}$.

In contrast, Figure 2 shows that $\#\mathcal{R}/\Pi$ remains greater than $2^\lambda$ even when the adversary selects a set $\mathcal{R}$ satisfying $\#\mathcal{R} = 1$, which constitutes the most favorable scenario for the adversary. Consequently, the proposed parameter choices preserve the security of POKÉ-4D.

## 6 Conclusion

In this study, we analyzed the security of POKÉ.

We showed that if the degree of the secret isogeny $\phi$ in the public key satisfies

$$D'^2 - \deg\phi = r \cdot c^2,$$

where $D'$ denotes the order of the specified torsion points, $r$ is a known integer, and $c$ is an unknown integer, then there exists a polynomial-time attack on POKÉ. In the POKÉ-2D setting, the probability that a public key of this form arises is bounded by $1/2^\lambda$, implying that such weak keys do not compromise the security of POKÉ-2D. Conversely, in the POKÉ-4D setting, this probability can exceed $1/2^\lambda$; therefore, these weak keys raise a security concern for POKÉ-4D.

We next considered a more generalized attack based on weak keys. Specifically, an adversary selects a set $\mathcal{R}$ of square-free integers and tests whether the target public key is a weak key corresponding to some $r \in \mathcal{R}$. The complexity of this attack is $\tilde{O}(\#\mathcal{R})$, and the associated success probability is $O(\sqrt{\#\mathcal{R}}/2^\lambda)$

for POKÉ-2D and $O(\sqrt{\#\mathcal{R}}/2^{\lambda/2})$ for POKÉ-4D. Therefore, while POKÉ-2D achieves $\lambda$-bit security, POKÉ-4D does not necessarily attain $\lambda$-bit security.

Finally, we proposed a new choice of parameters for POKÉ-4D to resist our weak-key attack. In particular, we recommend adopting the same parameter set as that of POKÉ-2D. Unfortunately, this adjustment eliminates the performance advantages that POKÉ-4D originally offered in comparison to POKÉ-2D.

## Acknowledgements

We thank the anonymous reviewers for their helpful feedback and constructive comments, which significantly improved the quality of this work. We also made use of a generative AI tool to assist with refining the English writing.

This work was supported by JSPS KAKENHI Grant Number JP25K24402.

## References

1. Marius A Aardal, Gora Adj, Diego F Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, et al. SQIsign 2.0: Algorithm specifications and supporting documentation. 2025.
2. Andrea Basso and Luciano Maino. POKÉ: A compact and efficient PKE from higher-dimensional isogenies. In *Advances in Cryptology – EUROCRYPT 2025*, pages 94–123. Springer, 2025.
3. Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: Fast encryption from supersingular torsion attacks. In *Advances in Cryptology – ASIACRYPT 2023*, pages 98–126. Springer, 2023.
4. Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *Proceedings of the Fourteenth Algorithmic Number Theory Symposium–ANTS 2020*, volume 4, pages 39–55. Mathematical Sciences Publishers, 2020.
5. Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International conference on cryptology in India*, pages 428–442. Springer, 2014.
6. Andrew R. Booker, Ghaith A. Hiary, and Jon P. Keating. Detecting squarefree numbers. *Duke Mathematical Journal*, 164(2):235 – 275, 2015.
7. Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, pages 423–447. Springer, 2023.
8. Pierrick Dartois. Fast computation of 2-isogenies in dimension 4 and cryptographic applications. *Journal of Algebra*, 2025.
9. Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQISignHD: new dimensions in cryptography. In *Advances in Cryptology – EUROCRYPT 2024*, pages 3–32. Springer, 2024.
10. Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.
11. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93. Springer, 2020.

12. Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, pages 425–440, 2016.
13. Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford university press, 1979.
14. Jonas Janneck, Jonas Meers, Massimo Ostuzzi, and Doreen Riepel. Snake Mackerel: An isogeny-based AKEM leveraging randomness reuse, 2025. `https://eprint.iacr.org/2025/1474`.
15. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography – PQCrypto 2011*, pages 19–34. Springer, 2011.
16. Ernst Kani. The number of curves of genus two with elliptic differentials. 1997.
17. Hyeonhak Kim, Seokhie Hong, Suhri Kim, and Sangjin Lee. INKE: Fast isogeny-based PKE using intermediate curves, 2025. `https://eprint.iacr.org/2025/1458`.
18. David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 148(5):1483–1515, 2012.
19. Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, pages 448–471. Springer, 2023.
20. Tomoki Moriya and Miha Stopar. LIT-SiGamal: An efficient isogeny-based PKE based on a LIT diagram. In *Advances in Cryptology – ASIACRYPT 2025*, pages 275–306. Springer, 2025.
21. National Institute of Standards and Technology. Post-quantum cryptography: Additional digital signature schemes. `https://csrc.nist.gov/projects/pqc-dig-sig/round-2-additional-signatures`.
22. Damien Robert. Breaking SIDH in polynomial time. In *Advances in Cryptology – EUROCRYPT 2023*, pages 472–503. Springer, 2023.
23. Joseph Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.
24. Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. A*, 273(5):238–241, 1971.