A Note on the Post-Quantum Security of Identity-Based Encryption on Isogenous Pairing Groups

Malte Andersch, Cezary Pilaszewicz and Marian Margraf
Fachbereich Mathematik und Informatik
Freie Universität Berlin
Berlin, Germany
e-mail: {malte.andersch | cezary.pilaszewicz | marian.margraf}@fu-berlin.de

***Abstract*—The development of cryptographic schemes that remain secure in the post-quantum era is an urgent challenge, particularly in light of the growing ubiquity of low-power devices and the looming threat of quantum computing. Identity-Based Encryption (IBE) offers a compelling alternative to traditional Public Key Infrastructures by simplifying key management, but most classical IBE schemes rely on number-theoretic assumptions that are vulnerable to quantum attacks. In response, Koshiba and Takashima proposed a novel approach based on *Isogenous Pairing Groups* (IPGs), claiming partial quantum resistance. In this work, we critically examine their construction and security claims and investigate the security in standard security notions. We show that the proposed scheme, despite its theoretical elegance, reduces to the Elliptic Curve Discrete Logarithm Problem (ECDLP) on supersingular curves, which can be broken in polynomial time by quantum algorithms in the IND-ID-CPA setting and in subexponential time classically in the authors' security models. Our analysis reveals structural weaknesses inherent to the IPG framework, such as the use of explicit group elements in prime-order groups and exploitable isogeny homomorphisms, which undermine the post-quantum security of isogeny-based cryptography. These findings suggest that IPG-based constructions, which use more than a single point per pairing group, are unlikely to provide robust post-quantum security. In Koshiba and Takashima's proposed IBE system, we can directly observe this when paying regard to not only the IBE's Master Secret Key but also Users' Secret Keys.**

Keywords-Identity-Based Encryption; Isogeny; Post-Quantum Cryptography; Isogenous Pairing Groups.

I. Introduction

In an increasingly connected and digital world, ensuring robust security has become a fundamental requirement in the design of modern information systems. The growing integration of low-power, resource-constrained devices - alongside the accelerating development of quantum computing - poses significant new challenges. These developments highlight the urgent need for cryptographic schemes that are both secure and efficient across a wide range of deployment environments.

Conventional Public Key Infrastructures, though well-established and secure, involve considerable overhead due to the need for certificate issuance, distribution, and validation. *Identity-Based Encryption* (IBE) addresses these limitations by allowing a User's Identity - such as an email address or device ID - to act directly as their public key, thereby eliminating the need for certificates and simplifying key management.

In such systems, a central authority known as the *Trusted Entity* (or *Private Key Generator*, PKG) holds a *Master Secret Key* (MSK) and uses it to derive Secret Keys for users based on their identities. This streamlined design is particularly attractive in applications like secure messaging, mobile platforms, hierarchical authorization systems, and direct device-to-device encryption. However, the centralized nature of IBE introduces a significant trade-off: the PKG can compute any User's Secret Key, which creates a single point of trust and potential vulnerability if the authority is compromised.

The foundational idea of IBE was first proposed by Shamir in 1985 [1], and later realized in a concrete pairing-based construction by Boneh and Franklin in 2001 [2]. Since then, many IBE schemes have emerged, relying on a variety of computational hardness assumptions ranging from number-theoretic problems to constructions based on lattices.

However, the arrival of quantum computing presents a critical threat to the security of some of these classical approaches. Quantum algorithms - most notably Shor's algorithm - can efficiently solve problems like factoring and discrete logarithms, which underpin the security of most traditional public key and IBE schemes. This renders them vulnerable in the face of a quantum-capable adversary.

In response, there has been a major shift toward the development of *Post-Quantum Cryptographic* (PQC) primitives - schemes designed to remain secure against both classical and quantum attacks. Designing IBE systems that are quantum-resistant remains a pressing challenge in this broader effort. Among the many emerging schemes, Koshiba and Takashima proposed a new framework for partially quantum secure systems called Isogenous Pairing Groups (IPGs) [3] alongside an IBE using these IPGs. We find their idea to be generally appealing and elegant. However, there are some serious doubts about the validity of their security claims in a more practical scenario than described by their new security models, especially when considering the security of the IBE's Users' Secret Keys. Thus, we aim to investigate the weaknesses of the proposed scheme and analyze whether its security goals can be upheld in more standard notions of security.

This paper is organized as follows: First, Section II introduces the necessary mathematical foundations used in this paper. Section III provides a general overview of IBE alongside the most common security definitions and assumptions. In Section IV, we present the IBE scheme proposed by Koshiba and Takashima, outline their security claims, and argue for a more thorough analysis in different security models than the

 ISBN: 978-1-68558-442-9

original authors' propositions. Finally, Section V highlights our attacks against the previously introduced scheme in the Chosen Plaintext Attack for IBE (ID-CPA) setting and the original authors' Payload-Hiding against Quantum adversaries (PH-PQ) setting and performs a complexity analysis of the presented attacks.

II. Preliminaries

For this paper, we consider elliptic curves in the following manner:

Definition 2.1. *Let E be an elliptic curve over the finite field $\mathbb{F}_{p^m}$ for p prime and an integer $m \geq 1$, given by a Weierstrass equation $E: y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^m}$. The set of $\mathbb{F}_{p^m}$-rational points on E is*

$$E(\mathbb{F}_{p^m}) = \{(x, y) \in \mathbb{F}_{p^m}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ denotes the point at infinity. Equipped with the chord-and-tangent addition law, $E(\mathbb{F}_{p^m})$ forms a finite abelian group with $\mathcal{O}$ as the neutral element.

A. Isogenies

Ever since the seminal work of Shamir introducing the notion of IBE in [1], elliptic curves have played a central role in the design of IBE systems, including prominent examples like the Boneh-Franklin scheme [2] and the Boneh-Boyen scheme [4]. These constructions largely depend on the hardness of problems related to scalar multiplication on elliptic curves and bilinear pairings. However, the advent of quantum computing threatens the foundational assumptions of these schemes, as quantum algorithms can solve the underlying Discrete Logarithm Problem (DLP) efficiently.

To address this, attention has shifted towards alternative cryptographic primitives which resist quantum attacks. One such promising candidate is the class of *isogenies* between elliptic curves. Although their use in cryptography is relatively recent, isogeny-based schemes have gained momentum due to their conjectured post-quantum security and the appealing advantage of compact key sizes, which is particularly beneficial in resource-constrained environments.

Definition 2.2. *Let K be a field and $\overline{K}$ its algebraic closure. Let E_1 and E_2 be elliptic curves over $\overline{K}$, with respective points at infinity $\mathcal{O}_{E_1}$ and $\mathcal{O}_{E_2}$. Then, an* isogeny *is a finite, non-constant morphism $\phi : E_1 \to E_2$ defined over $\overline{K}$ such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. If this morphism is also defined over K, we say that ϕ is an isogeny over K.*

While we do not delve into the mathematical theory underlying isogenies - see [5] for a thorough introduction - we do introduce the central computational problem that forms the security foundation of isogeny-based cryptography:

Problem 2.3 (General Isogeny Problem, [6])**.** *Given two elliptic curves E_1 and E_2 defined over a finite field K, with $\#E_1 = \#E_2$, where $\#E$ denotes the number of points on the curve E, find an isogeny $\phi : E_1 \to E_2$ defined over K.*

To date, Problem 2.3 is believed to be intractable even for quantum adversaries, particularly in the supersingular setting. In fact, its hardness is closely tied to the difficulty of computing the endomorphism ring of elliptic curves, a problem shown to be equivalent in certain cases [7].

B. Bilinear Pairings

As the original primitive used in the Boneh-Franklin IBE construction, *pairings* have gained a lot of attention not only in the world of IBEs but also in a new subbranch of cryptography, the *pairing-based cryptography*. For the main concept of Koshiba and Takashima's paper, the IPGs, we also need to briefly introduce pairings as their second component.

Definition 2.4. *Let G_1, G_2, G_T be cyclic groups. A* Pairing *is a map*

$$e : G_1 \times G_2 \to G_T,$$

satisfying the following properties:

- *e is bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $a, b \in \mathbb{Z}, (P, Q) \in G_1 \times G_2$,*
- *e is non-degenerate: $e(P, Q) \neq 1$ for some $(P, Q) \in G_1 \times G_2$,*
- *e is efficiently computable.*

For G_1, G_2, the additive notation is most commonly used, while we use multiplicative notation for G_T.

While the considerations work for any pairing, we will use the Weil pairing used by the original authors of [3], and thus we will mainly focus on this specific pairing's properties here.

Before exploring the Weil pairing itself, we first need to introduce the notion of *torsion subgroups*.

Definition 2.5. *Let $E(\mathbb{F}_{p^m})$ an elliptic curve, then $E(\overline{\mathbb{F}_{p^m}})$ is the group of points over the algebraic closure of $\mathbb{F}_{p^m}$. Let also $n \in \mathbb{N}_+$. Then the group*

$$E[n] = \{P \in E(\overline{\mathbb{F}_{p^m}}) \mid [n]P = \mathcal{O}\}$$

is called the n-torsion subgroup of E. The order of all points P in this group divides n.

Using these n-torsion subgroups, we can define the Weil pairing as follows:

Definition 2.6. *Let $E(\mathbb{F}_{p^m})$ be an elliptic curve with p prime and $n \in \mathbb{N}^+$ with $\gcd(n, p^m) = 1$. The Weil pairing is the map*

$$e : E[n] \times E[n] \to \overline{\mathbb{F}_{p^m}}.$$

Specifically, the Weil pairing maps to the set of all primitive n-th roots of unity over $\overline{\mathbb{F}_{p^m}}$.

Additionally, the Weil pairing also satisfies the following properties:

(*a*) *Identity*: $e(P, P) = 1$, for all $P \in E[n]$
(*b*) *Bilinearity*: as before
(*c*) *Alternation*: $e(P, Q) = e(Q, P)^{-1}$, for all $P, Q \in E[n]$
(*d*) *Non-degeneracy*: If $e(P_1, P_2) = 1$ for all $P_2 \in E[n]$, then $P_1 = \mathcal{O}$

(*e*) *Embedding Degree*: Let k be the smallest non-zero integer such that $p^{mk} \equiv 1 \mod n$. Then $E[n] \subseteq E(\mathbb{F}_{p^{mk}})$, and therefore $e(P_1, P_2) \in \mathbb{F}_{p^{mk}}$ for all $P_1, P_2 \in E[n]$

(*f*) *Endomorphism Interaction*: For all separable $\alpha \in End(E)$ and $S, T \in E[n]$ it holds

$$e(\alpha(S), \alpha(T)) = e(S, T)^{deg(\alpha)}.$$

To keep this paper concise, we will not delve into the construction and implementation of the Weil pairing and instead refer the interested reader to [8]. It is important to note that while e_n is commonly used to denote the Weil pairing for the n-torsion subgroup, we omit this index n and instead later on use the indices t to indicate the group the pairing belongs to.

C. Isogenous Pairing Groups

The notion of IPGs is first introduced by Koshiba and Takashima in [3]. Through the combination of isogenies and bilinear pairings, the authors aim to establish a framework for constructing IBEs, where the MSK is protected via quantum-safe isogenies and the individual messages are classically secure through pairing cryptography.

Before delving into the concrete definition of IBE schemes and the proposed IBE scheme using IPGs, we first formally define IPGs and outline the fundamental security assumptions.

Definition 2.7 (Isogenous Pairing Groups, Def. 4 in [3])**.** *IPGs are an array of length $t \geq 0$ of tuples $\left(\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t, \phi_t\right)$ together with a target group $\mathbb{G}_T$, where $\left(\mathbb{G}_t, \hat{\mathbb{G}}_t, e_t, \mathbb{G}_T\right)$ are asymmetric pairing groups of prime order q with pairings*

$$e_t : \mathbb{G}_t \times \hat{\mathbb{G}}_t \to \mathbb{G}_T,$$

$\hat{g}_t \in \hat{\mathbb{G}}_t$, isogeny $\phi_t : \mathbb{G}_0 \to \mathbb{G}_t$ and $g_t = \phi_t(g_0) \in \mathbb{G}_t$. For $t = 0$, the isogeny ϕ_0 is the identity function.

The IPGs' generator (Gen^{IPG}) generates a random instance as follows:

$$Gen^{\mathsf{IPG}}(1^\kappa, d) \to \Big(pk^{\mathsf{IPG}} := \Big((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t\in[0,d]}, \mathbb{G}_T\Big), \; sk^{\mathsf{IPG}} := (\phi_t)_{t\in[d]}\Big).$$

The IPGs satisfy the ***compatibility*** *property:*

$$g_T := e_0(g_0, \hat{g}_0) = e_t(g_t, \hat{g}_t) = e_t(\phi_t(g_0), \hat{g}_t) \neq 1, g_T \in \mathbb{G}_T$$

for all $t \in [1, d]$, and we require $\mathbb{G}_t \neq \hat{\mathbb{G}}_t$ for all $t \in [0, d]$.

Based on these IPGs, we can then outline the necessary security definitions for the proposed IBE scheme. The most fundamental one of these is the *Isogeny Problem on IPG*, transferring the general isogeny problem into the setting of IPG.

Problem 2.8 (Isogeny Problem on IPG, Def. 5 in [3])**.** *Let*

$$\Big(pk^{\mathsf{IPG}} := \Big((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T\Big), \; sk^{\mathsf{IPG}} := \phi_1\Big) \leftarrow Gen^{\mathsf{IPG}}(1^\kappa, 1).$$

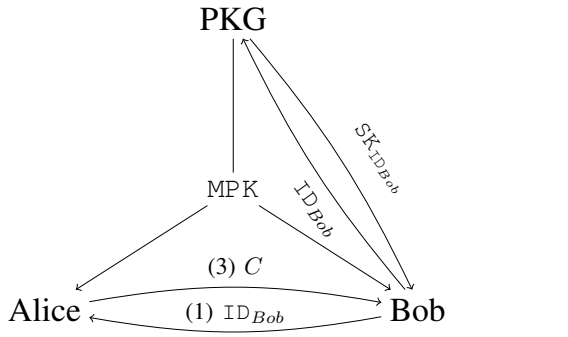

Figure 1. IBE Network Setup.

Given pk^{IPG}, find $sk^{\mathsf{IPG}} = \phi_1$.

Despite the additional inputs when compared to Problem 2.3 with $\mathbb{G}_0 \subseteq E_1(K)$, $\mathbb{G}_1 \subseteq E_2(K)$, Koshiba and Takashima claim Problem 2.8 to have no efficient quantum adversary.

III. Identity-Based Encryption

This section offers a general overview of the subject of IBE. We provide a definition of the necessary algorithms for IBE schemes and the IBE-related security games, as well as a brief discussion of the concept of pre-challenge quantum security in relation to the previously introduced IPGs.

A. Premise

The main challenge that IBE aims to overcome is the exchange of public keys, which is a fundamental part of traditional Public Key Infrastructures. The infrastructure of a typical IBE system is outlined in Figure 1. Here, Alice and Bob both retrieve the Master Public Key MPK from the PKG. When Alice wants to send an encrypted message to Bob, she uses Bob's User Identity $\mathtt{ID}_{Bob}$ and the MPK to encrypt the message M. Bob can retrieve his Secret Key $\mathtt{SK}_{\mathtt{ID}_{Bob}}$ from the PKG.

Definition 3.1. *An IBE scheme consists of four algorithms.*

- `setup`*: An algorithm that receives the security parameter as its input and creates the* `MPK` *and* `MSK`*.*
- `extract`*: An algorithm that uses the* `MPK`*,* `MSK` *and an Identity to generate the Secret Key corresponding to the Identity.*
- `encrypt`*: An algorithm that uses the* `MPK` *and an Identity to encrypt a message.*
- `decrypt`*: An algorithm that uses the* `MPK` *and a Secret Key corresponding to an Identity to decrypt a ciphertext into a message.*

B. Security Models on IBE

In the setting of IBE, classical security notions from Public Key Encryption (PKE) must be adapted to account for Identity-derived keys. The traditional definitions of Indistinguishability under adaptive Chosen Plaintext Attacks (IND-CPA) and

Chosen Ciphertext Attacks (IND-CCA) are extended to accommodate the fact that an adversary may obtain Secret Keys for multiple Identities $\texttt{ID}_1, \ldots, \texttt{ID}_n$, provided the challenge Identity remains hidden. Specifically, the attacker is allowed to query an extraction oracle $\mathcal{O}^{ext}(\texttt{ID})$ to obtain User's Secret Keys for arbitrary identities, except for the challenge Identity. We formalize this new CPA security for IBE (ID-CPA) via the following game-based definition:

Definition 3.2. *For an IBE scheme* $\Pi = (\mathtt{setup}, \mathtt{extract}, \mathtt{encrypt}, \mathtt{decrypt})$ *and a Probabilistic Polynomial-Time (PPT) adversary* $\mathcal{A}$*, the Indistinguishability under adaptive Chosen Plaintext Attack for IBE (IND-ID-CPA) game is defined as follows:*

Algorithm 1 IND-ID$^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game

Require: 1^κ the security parameter
1: $\texttt{extIDs} \coloneqq \emptyset$
2: $\texttt{MPK}, \texttt{MSK} \leftarrow \Pi.\texttt{setup}(1^\kappa)$
3: $\texttt{ID}^*, M_0, M_1 \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(ask, 1^\kappa, \texttt{MPK})$
4: $b \xleftarrow{\$} \{0,1\}$
5: $C_{\texttt{ID}^*} \leftarrow \Pi.\texttt{encrypt}(\texttt{MPK}, \texttt{ID}^*, M_b)$
6: $b' \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(guess, \texttt{MPK}, \texttt{ID}^*, C_{\texttt{ID}^*})$
7: **if** $\texttt{ID}^* \in \texttt{extIDs}$ **then**
8: **return** $\perp$
9: **end if**
10: **return** 1 iff $b' == b$

Figure 2. IND-ID-CPA game for IBE schemes.

For completeness, we also need to define the extraction oracle:

Algorithm 2 $\mathcal{O}^{ext}_{\Pi}(\texttt{ID})$

Require: ID the Identity to extract the Secret Key for
1: $\texttt{extIDs} \coloneqq \texttt{extIDs} \cup \{\texttt{ID}\}$
2: $\texttt{SK}_{\texttt{ID}} \leftarrow \Pi.\texttt{extract}(\texttt{MPK}, \texttt{MSK}, \texttt{ID})$
3: **return** $\texttt{SK}_{\texttt{ID}}$

Figure 3. Extraction Oracle for IBE security games.

We say that an IBE scheme has indistinguishable encryption under adaptive Chosen Plaintext Attack if, for any PPT adversary $\mathcal{A}$*, it holds that* $\mathcal{A}$*'s advantage* $Adv(\mathcal{A}) =: \varepsilon$ *in the success probability, defined as* $\Pr[\textit{IND-ID}^{cpa}_{\mathcal{A},\Pi}(\kappa) = 1] = \frac{1}{2} + \varepsilon$*, is negligible in* κ*.*

This definition can be extended to cover the IBE's Indistinguishability against Chosen Ciphertext Attacks (IND-ID-CCA) by providing the adversary with a decryption oracle, which, like the extraction oracle, rejects any query on the challenge Identity and ciphertext by returning $\perp$.

In addition to Indistinguishability-based (IND) notions, we consider a weaker but still meaningful security property: *One-wayness* (OW) of IBE schemes.

Definition 3.3. *For an IBE scheme* $\Pi = (\mathtt{setup}, \mathtt{extract}, \mathtt{encrypt}, \mathtt{decrypt})$ *and a PPT adversary* $\mathcal{A}$*, the One-wayness under adaptive Chosen Plaintext Attack for IBE (OW-ID-CPA) game is defined as follows:*

Algorithm 3 OW-ID$^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game

Require: 1^κ the security parameter
1: $\texttt{extIDs} \coloneqq \emptyset$
2: $\texttt{MPK}, \texttt{MSK} \leftarrow \Pi.\texttt{setup}(1^\kappa)$
3: $\texttt{ID}^* \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(ask, 1^\kappa, \texttt{MPK})$
4: $M \xleftarrow{\$} \mathcal{M}$
5: $C_{\texttt{ID}^*} \leftarrow \Pi.\texttt{encrypt}(\texttt{MPK}, \texttt{ID}^*, M)$
6: $M' \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(guess, \texttt{MPK}, \texttt{ID}^*, C_{\texttt{ID}^*})$
7: **if** $\texttt{ID}^* \in \texttt{extIDs}$ **then**
8: **return** $\perp$
9: **end if**
10: **return** 1 iff $M' == M$

Figure 4. OW-ID-CPA game for IBE schemes.

The extraction oracle is defined identically to the extraction oracle in the Indistinguishability game; see Algorithm 2.

We say that an IBE scheme provides One-wayness under adaptive Chosen Plaintext Attack if, for any PPT adversary $\mathcal{A}$*, it holds that* $\mathcal{A}$*'s advantage* $Adv(\mathcal{A}) =: \varepsilon$ *in the success probability, defined as* $\Pr[\textit{OW-ID}^{cpa}_{\mathcal{A},\Pi}(\kappa) = 1] = \varepsilon$*, is negligible in* κ*.*

Similar to the Indistinguishability scenario, the One-wayness can be extended to cover the CCA setting by incorporating a decryption oracle. While Indistinguishability is the de facto security standard for PKE schemes, the notion of One-wayness is especially relevant in our context. Any encryption scheme that satisfies One-wayness under CPA can be adapted to provide Indistinguishability under CCA via the Fujisaki-Okamoto transformation (FO-transform) [9]. This means that establishing One-wayness is often sufficient for constructing practically secure IBE schemes.

Naturally, Indistinguishability implies One-wayness: if an adversary can recover the plaintext from a ciphertext (as in the One-wayness game), they can also distinguish which message was encrypted (as in the IND game). In fact, a successful OW-ID-CPA adversary can be used as a subroutine in the IND-ID-CPA game by running it on the challenge ciphertext and comparing its output against the two original messages to guess the correct bit.

C. Pre-Challenge Quantum Security

Intuitively, the pre-challenge quantum security is aimed at protecting the MSK from quantum adversaries instead of the actual ciphertexts. This prevents an adversary from gaining classical access to the decryption of all ciphertexts via a single attack on the scheme with a quantum computer. Hence, allowing a quantum adversary to only decrypt ciphertexts one by one and thereby speculating upon the slow speed of introduction of powerful quantum computers. The cost of a

single attack is assumed to be high enough to mitigate the usefulness of early quantum machines against the scheme.

Using this assumption combined with the Decisional Bilinear Diffie-Hellman (DBDH) assumption [10], one obtains the following problem definition, used to prove the security of the proposed IBE scheme.

Problem 3.4 (qIsog-DBDH, Def. 7 in [3])**.** *Let $\mathcal{A} \coloneqq (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary, where $\mathcal{A}_1$ is modeled as a polynomial-time quantum adversary and $\mathcal{A}_2$ as a classical PPT machine. Let*

$$\Big(pk^{\mathsf{IPG}} \coloneqq \Big((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T\Big), \\ sk^{\mathsf{IPG}} \coloneqq \phi_1\Big) \leftarrow Gen^{\mathsf{IPG}}(1^\kappa, 1)$$

be generated by the IPG setup algorithm. Then:

- *$\mathcal{A}_1$ receives pk_{IPG} and outputs a state **state** $\leftarrow \mathcal{A}_1(pk_{\mathsf{IPG}})$.*
- *Next, random elements $\alpha, \beta, \delta \xleftarrow{\$} \mathbb{F}_q$ are sampled.*
- *$\mathcal{A}_2$ receives $\mathcal{X}_b$ for a uniformly chosen bit $b \xleftarrow{\$} \{0,1\}$, where $\mathcal{X}_0, \mathcal{X}_1$ are defined as the following tuples*

$$\mathcal{X}_0 \coloneqq \Big(\textbf{\textit{state}},\ g_0^\alpha,\ \hat{g}_1^\beta,\ g_T^{\alpha\beta}\Big), \\ \mathcal{X}_1 \coloneqq \Big(\textbf{\textit{state}},\ g_0^\alpha,\ \hat{g}_1^\beta,\ g_T^\delta\Big),$$

  with $g_T = e_0(g_0, \hat{g}_0) = e_1(\phi_1(g_0), \hat{g}_1) = e_1(g_1, \hat{g}_1)$.
- *$\mathcal{A}_2$ outputs a guess bit $b' \in \{0,1\}$.*

If $b = b'$, then the adversary $\mathcal{A} \coloneqq (\mathcal{A}_1, \mathcal{A}_2)$ wins*. The qIsog-DBDH assumption then states that for any adversary $\mathcal{A}$ as defined above, $\mathcal{A}$'s advantage for solving the qIsog-DBDH problem is negligible in κ.*

Koshiba and Takashima reduce Problem 3.4 to Problem 2.8, to show that a cryptosystem that is provably secure under the qIsog-DBDH assumption has no efficient adversary.

Applying the idea of pre-challenge quantum security to the established ID-CPA and ID-CCA notions of security, we replace the ask phase of the adversary $\mathcal{A}$ in the games defined in Algorithm 1 and Algorithm 3 with the quantum algorithm $\mathcal{A}_1$ and the $guess$ phases with the classical algorithm $\mathcal{A}_2$. We still assume all queries to the oracles in both phases to be only classical queries.

IV. IBE USING IPG

Using the notion of IPGs from Section II-C, Koshiba and Takashima introduce an IBE scheme that is supposedly resistant to pre-challenge quantum adversaries. In this section, we want to briefly introduce the scheme itself, alongside the original authors' security claims.

A. Scheme Description

Figure 5 contains the pseudocode for the implementation of the IBE on IPGs scheme. As before, we denote with $\mathbb{G}_t$ the cyclic symmetric pairing groups of prime order q exponential in κ on supersingular elliptic curves over a finite field $\mathbb{F}_{p^m}$.

Anonymous IBE using IPG approach

$\texttt{setup}\,(1^\kappa) \to (\texttt{MPK}, \texttt{MSK})$:
1) Generate IPG parameters:
$$\Big(\text{pk}^{\mathsf{IPG}} \coloneqq \Big((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T\Big), \\ \text{sk}^{\mathsf{IPG}} \coloneqq \phi_1\Big) \leftarrow \text{Gen}^{\mathsf{IPG}}(1^\kappa, 1).$$
2) Generate a random hash function $H : \mathbb{F}_q \to \mathbb{G}_0$ with $\mathbb{F}_q$ being the space of all possible Identities
3) Output $\texttt{MPK} \coloneqq (\text{pk}^{\mathsf{IPG}}, H)$, $\texttt{MSK} \coloneqq \text{sk}^{\mathsf{IPG}}$

$\texttt{extract}\,(\texttt{MPK}, \texttt{MSK}, \texttt{ID}) \to \texttt{SK}_{\texttt{ID}}$:
1) Calculate $h_0 \coloneqq H(\texttt{ID}) \in \mathbb{G}_0$ and $h_1 \coloneqq \phi_1(h_0)$
2) Output $\texttt{SK}_{\texttt{ID}} \coloneqq h_1$

$\texttt{encrypt}\,(\texttt{MPK}, \texttt{ID}, M) \to C_{\texttt{ID}}$:
1) Calculate $h_0 \coloneqq H(\texttt{ID})$
2) Generate a random exponent $\zeta \xleftarrow{\$} \mathbb{F}_q^\times$
3) Calculate $C \coloneqq \hat{g}_1^\zeta$ and $z \coloneqq e_0(h_0, \hat{g}_0)^\zeta$
4) Encrypt the plaintext as $C_T \coloneqq z \cdot M$
5) Output $C_{\texttt{ID}} \coloneqq (C, C_T)$

$\texttt{decrypt}\,(\texttt{MPK}, \texttt{SK}_{\texttt{ID}}, C_{\texttt{ID}'}) \to M$:
1) Calculate $z' \coloneqq e_1(h_1, C)$
2) Obtain the plaintext as $M' \coloneqq C_T \cdot (z')^{-1}$
3) Output $M \coloneqq M'$

Figure 5. Anonymous IBE against Pre-Challenge Quantum Adversaries proposed in [3].

The correctness of the algorithm for $\texttt{ID} == \texttt{ID}'$ follows from the IPG's compatibility property in Definition 2.7:

$$z' = e_1(h_1, C) = e_1(\phi_1(h_0), \hat{g}_1^\zeta) = e_1(\phi_1(h_0), \hat{g}_1)^\zeta \\ = e_0(h_0, \hat{g}_0)^\zeta = z.$$

The scheme in Figure 5 allows for the encryption of arbitrary messages $M \in \mathbb{F}_q$, thus the encryption of multiple bits. Meanwhile, the Secret Key size for each $\texttt{ID}$ is just a single element of $\mathbb{G}_0$, the ciphertext is the size of two elements of $\mathbb{G}_0$, and the public parameters are precisely the parameters for two elliptic curves. Compared to the Boneh-Franklin IBE, this is simply a doubling in size for the public parameters, while all other parameter sizes are equally large, giving an impression of practicality for the scheme.

B. The Original Authors' Claims

Koshiba and Takashima provide two security claims for the construction in Figure 5.

Claim 4.1 (Theorem 1. in [3])**.** *The proposed IBE scheme is Payload-Hiding against Quantum adversaries (PH-PQ) under Chosen Plaintext Attack under the qIsog-DBDH assumption in the quantum Random Oracle Model.*

While the PH-PQ security closely resembles the standard IND-ID-CPA security, there is a small distinction, in that the adversary must not query the challenge Identity to the mapping hash function H (implemented as a quantum accessible random oracle) in the pre-challenge phase. We present the definition of PH-PQ security in the appendix of the full version of this paper [11].

Besides Claim 4.1, Koshiba and Takashima also present another claim on a security notion they call Anonymous-ID (A-ID) security.

Claim 4.2 (Theorem 2. in [3])**.** *The proposed IBE scheme is A-ID secure against pre-challenge quantum adversaries under the qIsog-DBDH assumption in the quantum Random Oracle Model.*

Although this notion of security has little importance in literature for IBE schemes, we also want to provide its definition in the appendix of the full version of this paper [11].

Both these new notions can be put into perspective when introducing another notion of security, namely One-way Payload-Hiding against Quantum adversaries under Chosen Plaintext Attack (OW-PH-PQ-CPA); see Definition 4.3.

Definition 4.3. *For an IBE scheme* $\Pi = (\texttt{setup}, \texttt{extract}, \texttt{encrypt}, \texttt{decrypt})$ *and a PPT adversary* $\mathcal{A}$*, the OW-PH-PQ-CPA game is defined as follows:*

Algorithm 4 OW-PH-PQ$^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game

Require: 1^κ the security parameter
1: $\texttt{extIDs} \coloneqq \emptyset$
2: $\texttt{MPK}, \texttt{MSK} \leftarrow \Pi.\texttt{setup}(1^\kappa)$
3: $\texttt{ID}^* \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(ask, 1^\kappa, \texttt{MPK})$
4: $M^* \xleftarrow{\$} \mathbb{F}_q$
5: $C_{\texttt{ID}^*} \leftarrow \Pi.\texttt{encrypt}(\texttt{MPK}, \texttt{ID}^*, M^*)$
6: $M \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(guess, \texttt{MPK}, \texttt{ID}^*, C_{\texttt{ID}^*})$
7: **if** $\texttt{ID}^* \in \texttt{extIDs}$ **then**
8: **return** $\perp$
9: **end if**
10: **return** 1 iff $M == M^*$

Figure 6. OW-PH-PQ-CPA game for IBE schemes.

During the pre-challenge phase, the adversary is not allowed to query the challenge Identity to the hash function H, implemented as a quantum-accessible random oracle. The extraction oracle is defined identically to the extraction oracle in the Indistinguishability game (see Algorithm 2) and can only be queried classically.

We say that an IBE scheme is OW-PH-PQ secure under adaptive Chosen Plaintext Attack if, for any PPT adversary $\mathcal{A}$, it holds that $\mathcal{A}$'s advantage $Adv(\mathcal{A}) =: \varepsilon$ in the success probability, defined as $\Pr[\textit{OW-PH-PQ}^{cpa}_{\mathcal{A},\Pi}(\kappa) = 1] = \varepsilon$, is negligible in κ.

Based on the game defined in Definition 4.3, we present the following lemmas:

Lemma 4.4. *Let* $\Pi = (\texttt{setup}, \texttt{extract}, \texttt{encrypt}, \texttt{decrypt})$ *be a Payload-Hiding against Quantum adversaries IBE scheme, i.e., for every adversary $\mathcal{A}$ in the PH-PQ$^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game, it holds that $Adv(\mathcal{A}) \leq negl(\kappa)$ for some negligible function $negl(\cdot)$. Then it must hold for every adversary $\mathcal{A}'$ in the OW-PH-PQ$^{cpa}_{\mathcal{A}',\Pi}(\kappa)$ game, that $Adv(\mathcal{A}') \leq negl'(\kappa)$, for some negligible function $negl'(\cdot)$.*

Lemma 4.5. *Let* $\Pi = (\texttt{setup}, \texttt{extract}, \texttt{encrypt}, \texttt{decrypt})$ *be an A-ID secure IBE scheme, i.e., for every adversary $\mathcal{A}$ in the A-ID$^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game, it holds that $Adv(\mathcal{A}) \leq negl(\kappa)$ for some negligible function $negl(\cdot)$. Then it must hold for every adversary $\mathcal{A}'$ in the OW-PH-PQ$^{cpa}_{\mathcal{A}',\Pi}(\kappa)$ game that $Adv(\mathcal{A}') \leq negl'(\kappa)$, for some negligible function $negl'(\cdot)$.*

We prove Lemma 4.4 and Lemma 4.5 in the appendix of the full version of this paper [11].

Using Lemma 4.4 and Lemma 4.5, it becomes clear that any successful attack in the OW-PH-PQ game can directly be transformed into an attack on the claims by Koshiba and Takashima.

Furthermore, it is clear that these security notions are directly implied by the standard OW-ID-CPA security notions. Any attacker breaking OW-PH-PQ security can also be directly used to break OW-ID-CPA security. The only difference lies in the restricted oracle accessibility for the challenge Identity in the PH-PQ scenario, which, when lifted, does not affect the attacker's success probability.

We argue that the original authors' models, by restricting the calculation of the challenge Identity's public key, do not provide full practicality, as the direct calculation of a User's Public Key from their Identity is one of the main aspects of IBE. In practice, the restriction posed upon the hash function mapping the identities to public keys cannot be implemented.

Furthermore, while Koshiba and Takashima describe their intuition of pre-challenge quantum security as the adversary being only able to decrypt each ciphertext one-by-one, they simply reduce this to protecting the MSK and neglect the post-quantum security of the Users' Secret Keys. For these reasons, we want to extend their security analysis to the ID-CPA model in the pre-challenge quantum adversary setting in order to shed light on these aspects of the scheme's security.

V. Proposed Attacks against the IBE on IPGs

This section will give a brief introduction to the *Discrete Logarithm Problem* (DLP) on elliptic curves before outlining different attacks in a pre-challenge quantum setting and a classical setting.

A. Discrete Logarithm Problem on Elliptic Curves

In cryptography, one-way trapdoor functions form the basis for modern asymmetric ciphers. While it remains unclear whether those actually exist, several mathematically hard problems have been proposed as the foundation for such functions. One of these problems is the DLP.

Problem 5.1 (Discrete Logarithm Problem)**.** *Let $\mathbb{G}$ be a group, and let $x, y \in \mathbb{G}$ be elements such that y is in the subgroup generated by x. The DLP is the problem of determining an integer such that $x^d = y$.*

When working with elliptic curves, the group of points on the curve is typically denoted as additive and the d-fold scalar multiplication of a point P is written as $[d]P$. We can then reformulate this problem for the group of points on elliptic curves.

Problem 5.2 (Elliptic Curve Discrete Logarithm Problem)**.** *Let $E(\mathbb{F}_{p^m})$ be an elliptic curve, and let $P, Q \in E(\mathbb{F}_{p^m})$ be points such that Q is in the subgroup generated by P. The* Elliptic Curve Discrete Logarithm Problem *(ECDLP) asks to find an integer d satisfying $Q = [d]P$.*

To this day, the fastest known algorithms to solve the ECDLP classically are collision algorithms such as Pollard's Rho [12] boasting exponential runtimes ($\sqrt{p}$ for a curve group of order q in the case of Pollard's Rho). As no efficient classical attacks exist, the ECDLP forms the basis for many modern cryptographic algorithms, such as ECDSA [13] and ECDH [14] (based on a closely related hard problem).

B. Quantum Attack against the Discrete Logarithm Problem

The ECDLP can be solved efficiently on a quantum computer in the same way as was shown by Shor [15] for the DLP in multiplicative groups of cyclic groups of prime order. More precisely, the reason is that the ECDLP reduces to an instance of the hidden subgroup problem for finite abelian groups. Given $E(\mathbb{F}_{p^m})$ and $P, Q \in E(\mathbb{F}_{p^m})$ such that $Q = [k]P$ for some $k \in \mathbb{Z}$, and letting r be the order of P, the following function hides the subgroup generated by $(\overline{k}, \overline{-1}) \in \mathbb{Z}_r \times \mathbb{Z}_r$.

$$\begin{aligned} f \colon \mathbb{Z}_r \times \mathbb{Z}_r &\to E(\mathbb{F}_{p^m}) \\ (\overline{x}, \overline{y}) &\mapsto [x]P + [y]Q \end{aligned}$$

As shown in [16], there is a quantum algorithm that finds a generator of the hidden subgroup with probability at least $1 - \frac{1}{r}$ making $\mathcal{O}(\log(r))$ calls to f, along with efficiently computable quantum operations and classical post-processing that runs in time $\mathcal{O}(\log^2(r))$. The function f is efficiently computable by the standard double-and-add technique, ensuring that the overall procedure is. For an optimized way to implement f, see [17]. Moreover, from any generator found by the algorithm, k can be efficiently recovered.

C. Proposed Quantum Attack

We present our attack in the pre-challenge quantum OW-ID-CPA setting (see Definition 3.3), as this not only breaks the scheme's pre-challenge quantum IND-ID-CPA security but also highlights that the FO-transform is not directly applicable to this scheme. Therefore, there exists no simple way of achieving chosen-ciphertext security for the proposed scheme (see Section A for the scheme's CCA security).

For our attack, we aim to exploit the homomorphism property of the secret isogeny $\phi_1 : \mathbb{G}_0 \to \mathbb{G}_1$. As per the definition of homomorphism, it must hold for any $g \in \mathbb{G}_0, a \in \mathbb{Z}$ that $\phi_1(a \cdot g) = a \cdot \phi_1(g)$. Intuitively, the attack consists of two steps:

1) select a random Identity $\texttt{ID}^*$ as the challenge Identity and generate its hash $h^* = H(\texttt{ID}^*)$,
2) solve the ECDLP using Shor's algorithm for some x, such that $h^* = [x]g_0$.

This might fail if $h^* \notin \langle g_0 \rangle$, however, since $\mathbb{G}_0$ is cyclic of prime order, this can only occur if g_0 is the neutral element of $\mathbb{G}_0$. As g_0 is drawn at random from all $q \in 2^{O(n)}$ elements in $\mathbb{G}_0$ during the IPGs generation, this only happens with negligible probability. In Remark 5.3, we give an intuition on handling this case. Once we have obtained x, it must now also hold that if $h^* = [x]g_0$ then

$$\phi_1(h^*) = \phi_1([x]g_0) = [x]\phi_1(g_0) = [x]g_1.$$

We thus simply multiply the public g_1 by x and obtain the Secret Key $\texttt{SK}_{\texttt{ID}^*}$ for $\texttt{ID}^*$ without having queried it to the extraction oracle. Thus, we can select $\texttt{ID}^*$ as the challenge Identity and decipher any ciphertext encrypted under $\texttt{ID}^*$ classically in the post-challenge phase.

Formally, we construct a pre-challenge quantum attacker in the OW-ID-CPA game against the scheme, as shown in the following two algorithms. We assume Shor's algorithm for the ECDLP to be available as a subroutine $ECDLPShor(\cdot)$. We further assume the point $g_0 \neq \mathcal{O}_0$, i.e., the point g_0 from the $\texttt{MPK}$ is not the neutral element of $\mathbb{G}_0$.

Algorithm 5 $\mathcal{A}_1$

Require: $1^\kappa, \texttt{MPK}, \mathcal{O}^{ext}(\cdot)$
1: $\texttt{ID}^* \xleftarrow{\$} \mathbb{F}_q$
2: $h^* := H(\texttt{ID}^*)$
3: $d \leftarrow ECDPLShor(\mathbb{G}_0, g_0, h^*)$
4: $\texttt{SK}_{\texttt{ID}} := g_1$
5: $\texttt{SK}_{\texttt{ID}^*} := [d]\texttt{SK}_{\texttt{ID}}$
6: **return** $\texttt{ID}^*$

Figure 7. Pre-Challenge Quantum Adversary $\mathcal{A}_1$.

Remark 5.3. *We want to highlight that the attack is still very much possible if $g_0 = \mathcal{O}_0$: instead of using g_0 as the basis for the ECDLP, we instead generate another random $\texttt{ID}$ and issue a key extraction query for this Identity. We can then use $g_0 := H(\texttt{ID})$ and $g_1 \leftarrow \mathcal{O}^{ext}(\texttt{ID})$ for the attack.*

The classical part of the adversary obtains the Secret Key $\texttt{SK}_{\texttt{ID}^*}$ from this first algorithm. The complete algorithm is defined in Algorithm 6.

It should be evident that this adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ succeeds with probability $\Pr[\text{OW-ID}^{cpa}_{\Pi,\mathcal{A}}(\kappa) = 1] = 1 - \frac{1}{q}$. This stems from the fact that solving the ECDLP using Shor's algorithm for the Hidden Subgroup Problem succeeds with probability $1 - \frac{1}{ord(h^*)}$ (see Section V-B) and $ord(h^*) = q$ since $\mathbb{G}_0$ is cyclic of prime order q (see Section II-C). By the correctness assumption, it must hold that

Algorithm 6 $\mathcal{A}_2$

Require: $\texttt{MPK}, \mathcal{O}^{ext}(\cdot), \texttt{ID}^*, C_{\texttt{ID}^*}$
1: $M \leftarrow \Pi.\texttt{decrypt}(\texttt{MPK}, \texttt{SK}_{\texttt{ID}^*}, C_{\texttt{ID}^*})$
2: **return** M

Figure 8. Post-Challenge Classical Adversary $\mathcal{A}_2$.

$\Pi.\texttt{decrypt}(\texttt{MPK}, \texttt{SK}_{\texttt{ID}}, \Pi.\texttt{encrypt}(\texttt{MPK}, \texttt{ID}, M)) = M$ with probability 1. Runtime-wise, we expect the hash function, random selection, and scalar multiplication of curve points to run in constant time $\tilde{O}(1)$ and Shor's algorithm to run in time $O(\log^2(q))$.

It is also noteworthy that we managed to reconstruct a key for an arbitrary Identity without even possessing a single key-pair ourselves, and thus without querying the extraction oracle.

We acknowledge that this attack cannot be executed in the authors' PH-PQ security model. Nonetheless, this attack shows, that when provided access to the hash function H, as would be in a practical setting, a pre-challenge quantum adversary could reconstruct any User's Secret Key and thus decrypt any ciphertext addressed to them efficiently with a classical algorithm.

D. Proposed Classical Attack

Besides the quantum algorithm breaking the scheme's OW-ID-CPA pre-challenge quantum security in polynomial time, it is also possible to construct a classical adversary attacking the scheme's OW-PH-PQ (see Definition 4.3) security in subexponential time and therefore challenging both claims presented in Section IV-B. The idea here is generally the same as for the previous attack: solve the ECDLP, reconstruct the User's Secret Key for the challenge Identity, and use this key to decipher the challenge ciphertext. While the ECDLP is usually considered to be difficult to solve using classical means, we can exploit another property of the proposed scheme.

When working with isogenies as trapdoor homomorphisms, one usually uses supersingular elliptic curves, as these provide a more complex, expander-like isogeny graph, making it quantum-hard to navigate the graph and find secret isogenies. Furthermore, the endomorphism ring for supersingular elliptic curves forms a non-commutative quaternion algebra, which is also quantum-hard to compute. It is proven that finding an isogeny between two elliptic curves is as hard as computing their endomorphism ring [7]. Hence, the authors also propose using supersingular elliptic curves.

Now, as we have shown that an attack against this scheme is basically an attack against the ECDLP, we are facing another property of supersingular elliptic curves: their embedding degree is always $k \leq 6$, making them prone to the MOV attack [18]: Menezes et al. present a method of reducing the ECDLP for supersingular elliptic curves to the DLP in $\mathbb{F}_{p^{2k}}$. In this setting, we are no longer restricted to the use of collision algorithms (Pollard's Rho), which boast exponential runtime-complexities, but can instead use subexponential time algorithms such as the Index Calculus method [19]. Because of such attacks as the one presented in the following, NIST also recommends against the usage of supersingular elliptic curves (or curves with a small embedding degree in general) for classical ECDLP-based cryptography [20].

The attack itself follows the same scheme as the quantum attack in Section V-C. However, as we cannot query the challenge Identity in the pre-challenge phase for PH-PQ security, we instead only select a random challenge Identity in the first phase.

Algorithm 7 $\mathcal{A}_1$

Require: $1^\kappa, \texttt{MPK}, \mathcal{O}^{ext}(\cdot)$
1: $\texttt{ID}^* \xleftarrow{\$} \mathbb{F}_\text{q}$
2: **return** $\texttt{ID}^*$

Figure 9. Pre-Challenge Classical Adversary $\mathcal{A}_1$.

In the second phase, we then perform the same scheme of attack as in Algorithm 5.

Algorithm 8 $\mathcal{A}_2$

Require: $\texttt{MPK}, \mathcal{O}^{ext}(\cdot), \texttt{ID}^*, C_{\texttt{ID}^*}$
1: $h^* \coloneqq H(\texttt{ID}^*)$
2: $d \leftarrow \text{MOV-DLP}(\mathbb{G}_0, g_0, h^*)$
3: $\texttt{SK}_{\texttt{ID}} \coloneqq g_1$
4: $\texttt{SK}_{\texttt{ID}*} \coloneqq [d]\texttt{SK}_{\texttt{ID}}$
5: $M \leftarrow \Pi.\texttt{decrypt}(\texttt{MPK}, \texttt{SK}_{\texttt{ID}^*}, C_{\texttt{ID}^*})$
6: **return** M

Figure 10. Post-Challenge Classical Adversary $\mathcal{A}_2$.

To solve the ECDLP, instead of Shor's quantum algorithm for the ECDLP, we instead apply the MOV-reduction, described in Algorithm 9.

Algorithm 9 MOV-DLP

Require: $\mathbb{G}_0$ of order q on curve E_0, two points $g_o, h^* \in \mathbb{G}_0$
1: Determine k, c from [18, Table 1.]
2: $g' \xleftarrow{\$} E_0\left(\mathbb{F}_{p^{2k}}\right)$
3: $g \coloneqq \frac{c \cdot ord(g')}{q} \cdot g'$
4: $\alpha \coloneqq e_q(h^*, g)$
5: $\beta \coloneqq e_q(g_0, g)$
6: $x \leftarrow \text{NFS-DL}(\alpha, \beta)$
7: **return** x

Figure 11. DLP Algorithm using the MOV-Reduction.

Here, e_q denotes the Weil pairing on the q-torsion group of E_0. First, the ECDLP is reduced to the DLP in $\mathbb{F}_{p^{2k}}$ through the use of the Weil pairing. We then use the Number Field Sieve for Discrete Logarithms (NFS-DL) described in [21] from the Index Calculus family as a subroutine to solve the DLP in $\mathbb{F}_{p^{2k}}$. We expect the runtime of all operations except the NFS-DL to be in $\tilde{O}(1)$, while the Index Calculus boasts a

complexity of $L_{p^{2k}}\left(1/3, \sqrt[3]{64/9}\right)$. Since $q \in O(p)$, we can also write this as $L_{q^{2k}}\left(1/3, \sqrt[3]{64/9}\right)$, which is subexponential in the size of $\mathbb{G}_0$ for small values of k, such as those for supersingular elliptic curves.

The algorithm has a success probability of $\Pr[\text{OW-ID}^{cpa}_{\Pi,\mathcal{A}}(\kappa) = 1] = 1 - \frac{1}{q}$. The algorithm always succeeds unless $ord(\alpha) < q$ and the probability $\Pr[ord(\alpha) = q] = \frac{\varphi(q)}{q}$ since there are $\varphi(q) = q - 1$ many elements of order q in $\mathbb{F}_{p^{2k}}$ and there are q cosets of $\langle g_0 \rangle$ in $E[q]$.

VI. Conclusion

In this paper, we provided detailed pre-challenge quantum attacks in both the OW-ID-CPA setting and the OW-PH-PQ setting on the IBE scheme based on IPGs proposed by Koshiba and Takashima. By leveraging the fact that the scheme's security reduces to the ECDLP on supersingular elliptic curves, we were able to break the scheme in polynomial time $O(\kappa^2)$ using quantum algorithms in the OW-ID-CPA game and subexponential time $L_{p^{2k}}[1/3, \sqrt[3]{64/9}], k \leq 6$ classically in the OW-PH-PQ game. We argue that IPGs contain an inherent structural weakness in any (pre-challenge) quantum scenario: the pairings used in IPGs require the use of explicit group elements and cannot be directly applied to curves as a whole. However, while isogenies between supersingular elliptic curves provide quantum secure properties for cryptography, mapping these explicit points between the isogenous groups using isogenies does not necessarily. Since the groups are cyclic of prime order, all the elements are related to one another through the elliptic curve discrete logarithm, as all elements, apart from the neutral element, are generators of $\mathbb{G}_t$. Meanwhile, through the homomorphism property of isogenies between elliptic curves, and since $ord(\mathbb{G}_t) = q$ for all $t \in [0, d]$, all the IPGs must also be isomorphic to one another. This means any adversary capable of solving the ECDLP can determine the relation of two public points $\phi_t(P), \phi_t(Q) \in \mathbb{G}_t$ (here we consider ϕ_0 to be the identity function) and thus also the relation of their origin points' P, Q images under the isogenies ϕ'_t in every pairing group $\mathbb{G}_{t'}$ isogenous to $\mathbb{G}_t$. Hence, if a single secret isogenous point to a public point is known, every secret point in the same group for every public point can be calculated as well using Shor's algorithm on a quantum computer. Classically, the required use of supersingular elliptic curves for the isogenies also weakens the scheme's resistance against an attack on the discrete logarithm in these groups significantly.

References

[1] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., Berlin, Heidelberg: Springer, 1985, pp. 47–53, ISBN: 978-3-540-39568-3. DOI: 10.1007/3-540-39568-7_5.

[2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed., Berlin, Heidelberg: Springer, 2001, pp. 213–229, ISBN: 978-3-540-44647-7. DOI: 10.1007/3-540-44647-8_13.

[3] T. Koshiba and K. Takashima, "Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups," 2016, Accessed: Feb. 13, 2025. [Online]. Available: https://eprint.iacr.org/2016/1138, pre-published.

[4] D. Boneh and X. Boyen, "Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles," in *Advances in Cryptology - EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds., Berlin, Heidelberg: Springer, 2004, pp. 223–238, ISBN: 978-3-540-24676-3. DOI: 10.1007/978-3-540-24676-3_14.

[5] L. De Feo, "Mathematics of Isogeny Based Cryptography," Nov. 11, 2017, arXiv: 1711.04062 [cs], pre-published.

[6] S. D. Galbraith and F. Vercauteren, "Computational problems in supersingular elliptic curve isogenies," *Quantum Information Processing*, vol. 17, no. 10, p. 265, Oct. 2018, ISSN: 1570-0755, 1573-1332. DOI: 10.1007/s11128-018-2023-6.

[7] B. Wesolowski, "The supersingular isogeny path and endomorphism ring problems are equivalent," in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, Feb. 2022, pp. 1100–1111. DOI: 10.1109/FOCS52979.2021.00109.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics). New York, NY: Springer New York, 2009, vol. 106, ISBN: 978-0-387-09494-6. DOI: 10.1007/978-0-387-09494-6.

[9] E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," *Journal of Cryptology*, vol. 26, no. 1, pp. 80–101, Jan. 1, 2013, ISSN: 1432-1378. DOI: 10.1007/s00145-011-9114-1.

[10] Y. Yacobi, "A Note on the Bilinear Diffie-Hellman Assumption," 2002, Accessed: Jul. 16, 2025. [Online]. Available: https://eprint.iacr.org/2002/113, pre-published.

[11] M. Andersch, C. Pilaszewicz, and M. Margraf, "A Note on the Post-Quantum Security of Identity-Based Encryption on Isogenous Pairing Groups," 2025, Accessed: Feb. 18, 2026. [Online]. Available: https://eprint.iacr.org/2025/1439, pre-published.

[12] J. M. Pollard, "A monte carlo method for factorization," *BIT Numerical Mathematics*, vol. 15, no. 3, pp. 331–334, Sep. 1, 1975, ISSN: 1572-9125. DOI: 10.1007/BF01933667.

[13] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, Aug. 1, 2001, ISSN: 1615-5262. DOI: 10.1007/s102070100002.

[14] R. Haakegaard and J. Lang, "The Elliptic Curve Diffie-Hellman (ECDH)," [Online]. Available: http://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Haakegaard+Lang.pdf.

[15] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, ISSN: 0097-5397. DOI: 10.1137/S0097539795293172.

[16] S. Hallgren, A. Russell, and A. Ta-Shma, "Normal subgroup reconstruction and quantum computation using group representations," in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, ser. STOC '00, New York, NY, USA: Association for Computing Machinery, May 1, 2000, pp. 627–635, ISBN: 978-1-58113-184-0. DOI: 10.1145/335305.335392.

[17] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Info. Comput.*, vol. 3, no. 4, pp. 317–344, Jul. 1, 2003, ISSN: 1533-7146.

[18] A. Menezes, S. Vanstone, and T. Okamoto, "Reducing elliptic curve logarithms to logarithms in a finite field," in *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing - STOC '91*, New Orleans, Louisiana, United States: ACM Press, 1991, pp. 80–89, ISBN: 978-0-89791-397-3. DOI: 10.1145/103418.103434.

[19] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," in *20th Annual Symposium on Foundations of Computer Science (Sfcs 1979)*, Oct. 1979, pp. 55–60. DOI: 10.1109/SFCS.1979.2.

[20] L. Chen, D. Moody, A. Regenscheid, A. Robinson, and K. Randall, "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-186, Feb. 3, 2023, NIST SP 800–186. DOI: 10.6028/NIST.SP.800-186.

[21] R. Barbulescu, "Algorithms for discrete logarithm in finite fields," Ph.D. dissertation, Université de Lorraine, Dec. 5, 2013. Accessed: Jul. 30, 2025. [Online]. Available: https://hal.univ-lorraine.fr/tel-01750438.

APPENDIX

A. Another Note on CCA security

While the authors do not claim the scheme to be CCA secure, we still want to show a trivial attack breaking the cipher, when provided access to a decryption oracle. Notably, we choose to present this attack in the One-way ID-CCA setting, as breaking this weaker security notion also breaks the Indistinguishability by implication.

We construct the following classical attacker $\mathcal{A}$ in the OW-ID-CCA game:

Algorithm 10 $\mathcal{A}$, ask phase

Require: $1^\kappa, \texttt{MPK}, \mathcal{O}^{ext}(\cdot), \mathcal{O}^{dec}(\cdot)$

1: $\texttt{ID}^* \xleftarrow{\$} \mathbb{F}_q$
2: **return** $\texttt{ID}^*$

Figure 12. Pre-Challenge Phase Algorithm for Adversary $\mathcal{A}$.

In the pre-challenge phase, we simply choose a random Identity to attack. The challenger will then select a challenge plaintext M^* uniformly at random, encrypt it and send the resulting challenge-ciphertext back to the adversary $\mathcal{A}$ in the post challenge phase described in Algorithm 11.

Assuming the hash function H to run in $O(1)$, the attack boasts a runtime-complexity of $\tilde{O}(1)$. The attack's correctness

Algorithm 11 $\mathcal{A}$, $guess$ phase

Require: $\texttt{MPK}, \mathcal{O}^{ext}(\cdot), \mathcal{O}^{dec}(\cdot), C_{\texttt{ID}^*} = (C^*, C_T^*)$

1: $h_0 \coloneqq H(\texttt{ID}^*)$
2: $\overline{C} \coloneqq C^* \cdot \hat{g}_1$
3: $\overline{C}_T \coloneqq C_T^* \cdot e_0(h_0, \hat{g}_0)$
4: $\overline{M} \leftarrow \mathcal{O}^{dec}((\overline{C}, \overline{C}_T))$
5: **return** $\overline{M}$

Figure 13. Post-Challenge Phase Algorithm for Adversary $\mathcal{A}$.

can be proven by observing the following equality:

$$\begin{aligned}
\overline{M} &= \overline{C}_T \cdot (e_1(h_1, \overline{C}))^{-1} = \overline{C}_T \cdot (e_1(h_1, C \cdot \hat{g}_1))^{-1} \\
&= \overline{C}_T \cdot (e_1(h_1, \hat{g}_1^\zeta \cdot \hat{g}_1))^{-1} = \overline{C}_T \cdot (e_1(h_1, \hat{g}_1^{\zeta+1}))^{-1} \\
&= \overline{C}_T \cdot (e_1(h_1, \hat{g}_1)^{\zeta+1})^{-1} = \overline{C}_T \cdot (e_1(\phi_1(h_0), \hat{g}_1)^{\zeta+1})^{-1} \\
&= \overline{C}_T \cdot (e_0(h_0, \hat{g}_0)^{\zeta+1})^{-1} \\
&= C_T^* \cdot e_0(h_0, \hat{g}_0) \cdot (e_0(h_0, \hat{g}_0)^{\zeta+1})^{-1} \\
&= M^* \cdot e_0(h_0, \hat{g}_0)^\zeta \cdot e_0(h_0, \hat{g}_0) \cdot (e_0(h_0, \hat{g}_0)^{\zeta+1})^{-1} \\
&= M^* \cdot e_0(h_0, \hat{g}_0)^{\zeta+1} \cdot (e_0(h_0, \hat{g}_0)^{\zeta+1})^{-1} = M^*.
\end{aligned}$$

Furthermore, all the used variables, namely $h_0, \hat{g}_0, \hat{g}_1$, are publicly available. As we assume h_i and $\hat{g}_i$ to stem from distinct groups, the bilinear pairing will never degenerate to 1. We assume that $\hat{g}_1 \neq \hat{\mathcal{O}}_1$, where $\hat{\mathcal{O}}_1$ denotes the neutral element of $\hat{\mathbb{G}}_1$, as well as $e_0(h_0, \hat{g}_0) \neq 1$.in either case, the original scheme would break: the first would result in $\hat{g}_1^\zeta = \hat{g}_1$, therefore $e_1(h_1, C) = e_1(h_1, \hat{g}_1) = e_0(h_0, \hat{g}_0)$, which allows the calculation of z' and thus M without knowledge of ζ, while the latter would directly encode $C_T = M$ and therefore leak the plaintext. It must then always follow, that $(C^*, C_T^*) \neq (\overline{C}, \overline{C}_T)$; hence the decryption oracle never rejects the decryption query. This attack therefore succeeds with probability $\Pr[\text{OW-ID}^{cca}_{\Pi,\mathcal{A}}(1^\kappa) = 1] = 1$.

We acknowledge that ID-CCA-security could, in fact, be achieved by applying modifications such as the FO-transform [9] to the proposed scheme if it were OW-ID-CPA secure, as shown by Boneh and Franklin in [2]; a property which we dispute in Section V.