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

Cryptanalysis of a "Quantum-Annoying" IBE

Malte Andersch, Cezary Pilaszewicz, Marian Margraf
{malte.andersch | cezary.pilaszewicz | marian.margraf}@fu-berlin.de

April 11, 2026

Malte Andersch

Malte Andersch (he/him) received the bachelor's degree in IT-systems engineering from the Hasso-Plattner-Institut Potsdam, Germany, in March 2021 and the master's degree in computer science from the Freie Universität Berlin, Germany, in February 2025. He is currently a PhD student in the work group "Information Security" led by Marian Margraf at Freie Universität Berlin.

His current research is focused on the fields of post-quantum cryptography and (classical) cryptanalysis, with a special emphasis on identity-based encryption and signatures as well as cryptography using isogenies.

Overview

Aims and Contributions

Aims and Contributions of this Paper

Aims:

- Investigation of encryption algorithms relevant to migrating to quantum secure cryptography
- Identify weaknesses in newly proposed Identity-based encryption (IBE) schemes

Contributions:

- Show the vulnerability of a proposed IBE scheme, supposedly resistant against early quantum computers
- Evaluate the applicability of Koshiba and Takashima's IPG framework to PQ-scenarios

Pre-Challenge Quantum Security or "Quantum Annoyance"

Assumptions and General Idea

Assumption: The introduction of CRQC will be slow, and operations will be expensive.

Idea:

- For a transitional period, it is infeasible to perform a large amount of QC operations
- Systems should withstand quantum attacks that enable classical breaks afterward
- In the context of PKE: QC may break individual messages, but not generate keys so that messages can be decrypted classically

Identity-Based Encryption

The IBE Idea

Identity-Based Encryption

IBE is a class of PKE schemes, using a unique identifier (e.g., `bob@example.com`) directly as the Entity's Public Key [1], thus eliminating the need for certificate management.

- A trusted authority, the **Private Key Generator (PKG)**, generates User Secret Keys
- Users obtain their Secret Keys after authentication

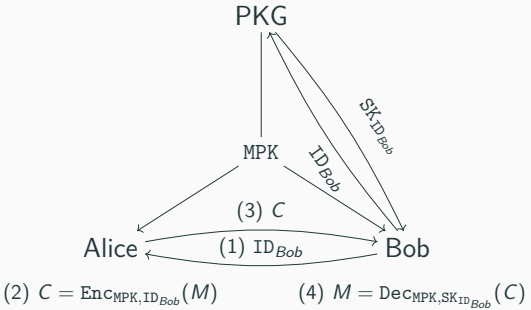

Figure 1: IBE Network Setup and Communication Example.

IBE Scheme Algorithms

IBE uses a set of four algorithms:

setup

- Input: Security Parameter 1^κ
- Output: MPK, MSK

extract

- Input: MPK, MSK, ID
- Output: $\mathtt{SK}_{\mathtt{ID}}$

encrypt

- Input: MPK, ID, message M
- Output: Ciphertext C

decrypt

- Input: MPK, $\mathtt{SK}_{\mathtt{ID}}$, C
- Output: Plaintext M

Security Model for IBE

Algorithm 1 **Classical** $\text{OW-ID}^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game

Require: 1^κ the security parameter

$\texttt{extIDs} := \emptyset$
$\texttt{MPK}, \texttt{MSK} \leftarrow \Pi.\texttt{setup}(1^\kappa)$
$\texttt{ID}^* \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(\textbf{ask}, 1^\kappa, \texttt{MPK})$
$M \xleftarrow{\$} \mathcal{M}$
$C_{\texttt{ID}^*} \leftarrow \Pi.\texttt{encrypt}(\texttt{MPK}, \texttt{ID}^*, M)$
$M' \leftarrow \mathcal{A}^{\mathcal{O}^{ext}(\cdot)}(\textbf{guess}, \texttt{MPK}, \texttt{ID}^*, C_{\texttt{ID}^*})$
if $\texttt{ID}^* \in \texttt{extIDs}$ **then**
    return $\perp$
end if
return 1 iff $M' == M$

Following the IND-ID-CPA games described in [2].

- $\Pi = (\texttt{setup}, \texttt{extract}, \texttt{encrypt}, \texttt{decrypt})$ is the IBE scheme
- $\mathcal{A}$ is a stateful **classical** PPT adversary
- $\mathcal{A}$ has **two phases**:
  - **ask**: $\mathcal{A}$ receives public parameters and selects a challenge Identity $\texttt{ID}^*$
  - **guess**: $\mathcal{A}$ receives the challenge ciphertext C^* and guesses the corresponding plaintext
- $\mathcal{A}$ is not allowed to extract the Secret Key $\texttt{SK}_{\texttt{ID}^*}$ for its chosen challenge Identity $\texttt{ID}^*$
- $\mathcal{A}$ wins, iff it can find the encrypted plaintext
- The scheme Π is secure iff $\mathcal{A}$ can only win with negligible probability

Security Model for IBE

Algorithm 2 Pre-Challenge Quantum $\text{OW-ID}^{cpa}_{\mathcal{A},\Pi}(\kappa)$ game

Require: 1^κ the security parameter

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

- $\Pi = (\texttt{setup}, \texttt{extract}, \texttt{encrypt}, \texttt{decrypt})$ is the IBE scheme
- $\mathcal{A}$ is a stateful **hybrid** PPT adversary
- $\mathcal{A} = (\mathcal{A}_{\mathbf{Q}}, \mathcal{A}_{\mathbf{C}})$ consists of **two algorithms**:
  - $\mathcal{A}_{\mathbf{Q}}$: **Quantum** algorithm selecting a challenge Identity $\texttt{ID}^*$
  - $\mathcal{A}_{\mathbf{C}}$: **Classical** algorithm receiving some **state** from $\mathcal{A}_{\mathbf{Q}}$ and C^* and guessing the corresponding plaintext
- $\mathcal{A}$ is not allowed to extract the Secret Key $\texttt{SK}_{\texttt{ID}^*}$ for its chosen challenge Identity $\texttt{ID}^*$
- $\mathcal{A}$ wins, iff it can find the encrypted plaintext
- The scheme Π is secure iff $\mathcal{A}$ can only win with negligible probability

IBE on Isogenous Pairing Groups

Elliptic Curves [3]

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.

Takeaways:

- $(E(\mathbb{F}_{p^m}), +)$ is an abelian group, points have coordinates in $\mathbb{F}_{p^m}^2$
- $\mathcal{O}$ is a point at infinity, functioning as the neutral element

Isogenies

Isogeny [4]

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.

General Isogeny Problem [5]

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.

The **General Isogeny Problem** for supersingular elliptic curves is considered to be intractable even for quantum adversaries [6].

Isogenous Pairing Groups

Bilinear Pairings

Let $\mathbb{G}, \hat{\mathbb{G}}$ be cyclic groups on elliptic curves and $\mathbb{G}_T$ another cyclic group. A **Pairing** is a map

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

satisfying (among others) the following properties:

- **Bilinearity**: $e(aP, bQ) = e(P, Q)^{ab}$ for all $a, b \in \mathbb{Z}, (P, Q) \in \mathbb{G} \times \hat{\mathbb{G}}$,
- **Non-degeneracy**: $\forall_{P \in \mathbb{G}} : e(P, Q) = 1 \implies P = \mathcal{O}$.

Isogenous Pairing Groups [7]

IPGs are an array of length $t \geq 0$ of tuples $\left(\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t, \phi_t\right)$ 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

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

an isogeny $\phi_t : \mathbb{G}_0 \to \mathbb{G}_t$ and elements $\hat{g}_t \in \hat{\mathbb{G}}_t$, $g_t = \phi_t(g_0) \in \mathbb{G}_t$.

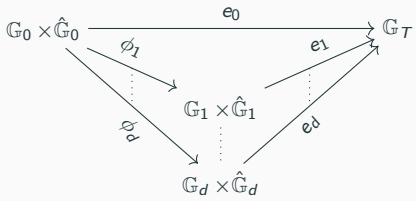

Figure 2: Compatibility of IPGs

Compatibility: for all $t \in [1, d]$:

$$g_T := e_0(g_0, \hat{g}_0) = e_t(g_t, \hat{g}_t) = e_t(\phi_t(g_0), \hat{g}_t)$$

Generator:

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

The Koshiba-Takashima IBE on IPGs [7]

$\texttt{setup}(1^\kappa) \to (\texttt{MPK}, \texttt{MSK})$:

1. Generate IPG parameters:

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

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 $\texttt{MPK} := (\mathsf{pk}^{\mathsf{IPG}}, H)$, $\texttt{MSK} := \mathsf{sk}^{\mathsf{IPG}}$

$\texttt{extract}(\texttt{MPK}, \texttt{MSK}, \texttt{ID}) \to \texttt{SK}_{\texttt{ID}}$:

1. Calculate $h_0 := H(\texttt{ID}) \in \mathbb{G}_0$ and $h_1 := \phi_1(h_0)$
2. Output $\texttt{SK}_{\texttt{ID}} := h_1$

$\texttt{encrypt}(\texttt{MPK}, \texttt{ID}, M) \to C_{\texttt{ID}}$:

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

$\texttt{decrypt}(\texttt{MPK}, \texttt{SK}_{\texttt{ID}}, C_{\texttt{ID}'}) \to M$:

1. Calculate $z' := e_1(h_1, C)$
2. Obtain the plaintext as $M' := C_T \cdot (z')^{-1}$
3. Output $M := M'$

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

Main Results

Core Observation

- In an IBE, the hash function $H(\cdot)$ is well-defined and public information
- We thus always have access to $\mathtt{PK}_{\mathtt{ID}} = H(\mathtt{ID}) = h^{\mathtt{ID}}$ for every $\mathtt{ID}$
- As User U with Identity $\mathtt{ID}_U$, we have access to private key $\mathtt{SK}_{\mathtt{ID}_U} = \phi_1\left(h^U\right)$
- Isogenies ϕ are homomorphisms of points on elliptic curves
- Groups in IPGs are cyclic of prime order
- For any attacked identity $\mathtt{ID}^*$:

$$ECDLP\left(\mathtt{PK}_{\mathtt{ID}^*}, \mathtt{PK}_{\mathtt{ID}_U}\right) = ECDLP\left(h^*, h^U\right) \approxeq ECDLP\left(\phi_1(h^*), \phi_1\left(h^U\right)\right) = ECDLP\left(\mathtt{SK}_{\mathtt{ID}^*}, \mathtt{SK}_U\right)$$

Quantum Attack

- In the quantum setting, the classical DLP can be solved using an algorithm proposed by Shor in [8]
- The algorithm can be adjusted to solve the Elliptic Curve DLP in polynomial time
- The full algorithm runs in $O(\log^2(q))$
- This attack cannot be executed in the authors' PH-PQ security model; as they disallow acces to $H(\cdot)$
  - However, in a real scenario public access to the hash function H enables it

Quantum Attack

Algorithm 3 Pre-Challenge Quantum $\mathcal{A}_{\mathbf{Q}}$

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

1: $\mathtt{ID}^* \xleftarrow{\$} \mathbb{F}_q$
2: $h^* := H(\mathtt{ID}^*)$
3: $d \leftarrow$ **ECDLPShor**$(\mathbb{G}_0, g_0, h^*)$
4: $\mathtt{SK}_{\mathtt{ID}} := g_1$
5: $\mathtt{SK}_{\mathtt{ID}^*} := [d]\mathtt{SK}_{\mathtt{ID}}$
6: **return** $\mathtt{ID}^*$

Algorithm 4 Post-Challenge Classical $\mathcal{A}_{\mathbf{C}}$

Require: $\mathtt{MPK}, \mathcal{O}^{ext}(\cdot), \mathtt{ID}^*, C_{\mathtt{ID}^*}$

1: $M \leftarrow \Pi.\mathtt{decrypt}(\mathtt{MPK}, \mathtt{SK}_{\mathtt{ID}^*}, C_{\mathtt{ID}^*})$
2: **return** M

Note: This attack requires us to have access to $H(\cdot)$ in the Pre-Challenge Phase

Classical Attack

- ECDLP is usually considered to be difficult in the classical setting
- Best algorithms for ECDLP are collision algorithms, which run in $O(\sqrt{q})$
- However, for supersingular elliptic curves, the embedding degree is always small, making them prone to the MOV attack [9]
  - They present a method of reducing the **supersingular elliptic curves DLP** to the **DLP in** $\mathbb{F}_{p^{2k}}$
  - There we can use more effective techniques like the Number Field Sieve [10]
- The full algorithm runs in $L_{q^{2k}}\left(1/3, \sqrt[3]{64/9}\right)$, which is subexponential in the size of κ for small embedding degrees

Classical Attack

Algorithm 5 Classical $\mathcal{A}$, **ask**-Phase

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

1: $\mathtt{ID}^* \xleftarrow{\$} \mathbb{F}_q$

2: **return** $\mathtt{ID}^*$

Note: We move the DLP into the Post-Challenge Phase to show that this attack even works with restricted acces to $H(\cdot)$

Algorithm 6 Classical $\mathcal{A}$ **guess**-Phase

Require: $\mathtt{MPK}, \mathcal{O}^{ext}(\cdot), \mathtt{ID}^*, C_{\mathtt{ID}^*}$

1: $h^* := H(\mathtt{ID}^*)$

2: $d \leftarrow$ **MOV-DLP**$(\mathbb{G}_0, g_0, h^*)$

3: $\mathtt{SK}_{\mathtt{ID}} := g_1$

4: $\mathtt{SK}_{\mathtt{ID}*} := [d]\mathtt{SK}_{\mathtt{ID}}$

5: $M \leftarrow \Pi.\mathtt{decrypt}(\mathtt{MPK}, \mathtt{SK}_{\mathtt{ID}^*}, C_{\mathtt{ID}^*})$

6: **return** M

Conclusion

Our Results

- Scheme is vulnerable to **key-recovery attacks** for individual Users
- **Pre-Challenge Quantum** adversary breaks the scheme in polynomial time $O(\log^2(q)) = O(\kappa^2)$
- **Classical** Adversary breaks the scheme in subexponential time $L_{q^{2k}}[1/3, \sqrt[3]{64/9}], k \leq 6$ for $q \in O(2^\kappa)$
- Fundamental weakness of explicit points in isogeny-based schemes further proven
- Classical weakness of supersingular EC for the ECDLP further proven

Literature i

[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] 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.

[4] L. De Feo, **"Mathematics of Isogeny Based Cryptography,"** arXiv: 1711.04062 [cs], pre-published.

Literature ii

[5] 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.

[6] 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.

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

[8] 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.

Literature iii

[9] 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.

[10] 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.