A Tightly Secure Identity-based Signature Scheme from Isogenies

Hyungrok Jo[1], Shingo Sato[1], and Junji Shikata[1,2]

[1] Institute of Advanced Sciences, Yokohama National University, Yokohama, Japan
[2] Graduate School of Environment and Information Sciences,
Yokohama National University, Yokohama, Japan
jo-hyungrok-xz@ynu.ac.jp, sato-shingo-zk@ynu.ac.jp, shikata-junji-rb@ynu.ac.jp

Abstract. We present a tightly secure identity-based signature (IBS) scheme based on the supersingular isogeny problems. Although Shaw and Dutta proposed an isogeny-based IBS scheme with provable security, the security reduction is non-tight. For an IBS scheme with concrete security, the tightness of its security reduction affects the key size and signature size. Hence, it is reasonable to focus on a tight security proof for an isogeny-based IBS scheme.
In this paper, we propose an isogeny-based IBS scheme based on the lossy CSI-FiSh signature scheme and give a tight security reduction for this scheme. While the existing isogeny-based IBS has the square-root advantage loss in the security proof, the security proof for our IBS scheme avoids such advantage loss, due to the properties of lossy CSI-FiSh.

1 Introduction

Post-Quantum Cryptography (PQC, for short) is a next-generation cryptographic system that differs from widely used cryptographic systems based on the hardness of integer factorization problems, and is globally popularized and used. It is based on various mathematically hard problems that are resistant to attacks by Shor's quantum algorithm [28] and has been actively researched by many researchers. Isogeny-based cryptography is one of the promising candidates for PQC, along with lattice-based cryptography, code-based cryptography, multivariate-based cryptography, and hash-based cryptography. National Institute of Standards and Technology (NIST) is currently in the process of standardizing practical post-quantum cryptography with sufficient security and practicality to promote and use these next-generation cryptographic systems in the near future. According to the results [21] announced in the third round released in July 2022, CRYSTALS-Kyber was selected for the KEM category and CRYSTALS-Dilithium, Falcon, and SPHINCS+ were selected for the signature category in the process of standardizing post-quantum cryptography. In particular, in the KEM category, BIKE, Classic McEliece, and HQC, as well as SIKE based on the hardness of supersingular isogeny problem, entered the fourth round. However, SIKE was unfortunately excluded from the candidates due to several attacks [7,20,24] known in September 2022. Since the fundamental computational hardness problem in isogeny-based cryptographic systems has not been solved yet, so cryptographic systems like CSIDH [8] and SQI-Sign [13] that do not rely on auxiliary point information in their basic structure, or have a different cryptographic construction than SIDH, continue to be considered secure. Recently, primeSIDH [19] and M(D)-SIDH [15] have also been introduced as isogeny-based cryptographic systems that are assumed to resistant to attacks on SIDH, so the legacy of isogeny-based cryptographic systems continues to evolve.

Meanwhile, isogeny-based cryptographic system is often considered less practical compared to other cryptographic systems, which has led to a limited number of proposals [5,22,27] for advanced functional isogeny-based encryption schemes. Nevertheless, from the essential perspective of identity-based cryptography, isogeny-based cryptographic systems can be advantageous in constructing identity-based schemes due to their compact key size compared to other PQC candidates. When a user joins a network, it can be particularly advantageous for identity-based cryptosystems, as the Key Generation Center (KGC) issues the master key and user key based on the user's identity (e-mail, social security number, credit card number, smart card, MAC address, IO/EO etc.) and then is not involved in the subsequent process.

Identity-Based Signatures from the CSIDH setting Shamir [26] suggested the first identity-based signature schemes, which are signature schemes with the public key of a user as his/her identity. Instead of

conducting the role of Public Key Infrastructures (PKI), a trusted KGC issues the corresponding secret key. CSIibs, proposed by Peng et al. [22], is the first identity-based signature scheme based on the supersingular isogeny assumption. However, Shaw and Dutta [27] pointed out a flaw in the main structure of CSIibs and proposed a new identity-based signature scheme based on supersingular isogeny assumption that includes the forward secrecy feature to address the issue. Both Peng et al. and Shaw and Dutta's identity-based signature schemes are based on CSIDH and use SeaSign [12] and CSI-FiSh [6] as their ID protocols.

CSI-FiSh and Lossy CSI-FiSh Isogeny-based cryptography was initially proposed by Couveignes [10] and by Rostovtsev and Stolbunov [25]. These proposals are known to be weakened by the quantum attack of Childs, Jao and Soukarev [9] against their based hardness assumptions on isogeny between ordinary elliptic curves. Instead of ordinary ellitic curves, Jao and De Feo [18] and Castryck et al. [8] proposed the Diffie-Hellman key exchanges using supersingular elliptic curves. As mentioned above, SIDH was broken by mainly Castryck and Decru [7] and subsequently Robert [20], Maino and Martindale [24]. These attacks do not apply to CSIDH-based schemes as SeaSign [12], CSI-FiSh [6], CSI-RAShi [4], Sashimi [11] and CSI-SharK [2]. Kaafarani et al. [14] proposed the lossy version of CSI-FiSh to achieve the tight reduction.

Our contributions We suggest the identity-based signature (IBS) scheme from isogenies with tight security.

The existing isogeny-based IBS scheme with provable security is the CSI-FiSh-based scheme proposed by Shaw and Dutta [27]. However, their scheme does not achieve tight security. This one is constructed by applying their proposed identity-based identification scheme to the Fiat-Shamir transformation. In order to prove the security of this IBS, it is necessary to employ the *forking lemma* and adaptive re-programming of random oracles [23,3]. Because of this, the security reduction for the existing one is not tight.

In order to construct an isogeny-based IBS scheme with tight security, our proposed scheme is based on lossy CSI-FiSh [14] which is a lossy identification scheme based on CSI-FiSh. Due to the result of [1], it is known that we can construct a signature scheme with tight security by applying a lossy identification scheme to the Fiat-Shamir transformation. Hence, it is reasonable to utilize lossy CSI-FiSh in order to construct a tightly secure IBS scheme.

Technical Overview. Although the construction of our proposed IBS is similar to that of the existing IBS [27], the security proof for ours is not obvious. To prove the security for a signature scheme constructed from a lossy identification scheme, we employ the following properties required to that identification scheme: *Indistinguishability of keys* and *lossy soundness*. A lossy identification scheme has two key generation algorithms: The ordinary (public-secret) key generation and *lossy key generation* which produces a (public) lossy key which is impossible to distinguish from a real public key. When a generated public key is lossy (called *lossy mode*), *lossy soundness* ensures that generating a valid response to a random challenge is statistically impossible after producing a commitment. When proving the security for a signature scheme from a lossy identification scheme, we replace a real public key with a lossy key by utilizing the standard hybrid argument (i.e., the sequence-of-games approach). However, we cannot employ lossy soundness in the straightforward way, when proving the security for our IBS scheme. This is because regarding IBSs, there is no notion corresponding to the lossy mode. Since an IBS scheme does not generate any public-secret key pair, we cannot employ the proof approach of [1].

In order to resolve this, we utilize the proof technique similar to the technique used for a tight security reduction of a DDH-based IBS scheme [16]. Regarding our proposed scheme, the key derivation algorithm produces a signature on an identity as a user secret key, and the signing algorithm generates a signature on an identity-message pair. These signatures are generated by using (a variant of) a lossy CSI-FiSh-based signature scheme. Informally, to prove the security, we simulate those signatures (i.e., those user secret key and signature on an identity and a message) without using a secret key of lossy CSI-FiSh. This is possible by utilizing a property of lossy CSI-FiSh and the sequence-of-games proof approach. Namely, we can replace real signatures with signatures generated in a lossy mode-like way, via tight security reductions. Hence, it is possible to give a tight security proof for our IBS scheme, by employing properties of lossy CSI-FiSh.

Comparison. We give a comparison of isogeny-based IBS schemes, in terms of key-size, signature-size, and security bound. Table 1 shows this comparison. From this table, we see that our security proof for the proposed scheme is significantly tighter compared to that for the existing one. Furthermore, the asymptotic MPK-size, USK-size, and signature-size of ours are equivalent to those of the existing scheme. This indicates

Table 1. Comparison of Isogeny-based IBS schemes

Scheme	MPK-Size	USK-Size	Signature-Size	Security Bound
[27]	$S_0\lceil\log p\rceil$	$T_1S_1(\lceil\log S_0\rceil + \lceil\log N\rceil)$	$T_1S_1\lceil\log p\rceil + T_1T_2(\lceil\log S_1\rceil + \lceil\log N\rceil)$	$\sqrt{q\cdot\epsilon} + \mathsf{negl}$
Our Scheme	$S_0\lceil\log p\rceil$	$T_1S_1(\lceil\log p\rceil + \lceil\log N\rceil)$	$T_1S_1\lceil\log p\rceil + T_1T_2(\lceil\log S_1\rceil + \lceil\log N\rceil)$	$S_0\cdot\epsilon + \mathsf{negl}$

We assume that the above IBS schemes use supersingular curves over $\mathbb{F}_p$. N is an odd order of an ideal cyclic group. ϵ is the maximum probability of breaking the underlying computational problem, and q is the maximum number of queries issued to (random) oracles. negl is a negligible function in a security parameter. S_0, S_1 are parameters of the corresponding computational assumptions. T_1, T_2 are the numbers of parallel executions of the underlying (lossy) identification scheme.

that these sizes of ours are also improved under a concrete security such as bit-security, since the security bound of our scheme is tighter. Hence, our goal is achieved, and we can claim that the key-size and signature-size of our scheme are better than those of the existing one, under concrete bit-security.

This paper is organized as follows. In section 2, we give the preliminaries for the CSIDH setting, lossy identification schemes, identity-based signatures and hardness assumptions. In section 3, we describe the construction of the lossy CSI-FiSh by [14]. In section 4, we suggest the tightly secure identity-based signature from the lossy CSI-FiSh.

2 Preliminaries

2.1 Elliptic curve and Ideal class group

We give some notations and preliminaries for using the CSIDH setting, which is based on [29,8,14]. Let E be an elliptic curve over a finite field $\mathbb{F}_p$ with a prime $p \geq 5$, and O_E denote the point at infinity on E. Let E and E' be the two elliptic curves over $\mathbb{F}_p$. It is called an *isogeny* φ between E and E' if $\varphi : E \to E'$ is a non-constant morphism satisfying $\varphi(0_E) = 0_{E'}$. A *separable* isogeny (it induces a separable extension of function fields) having $\{0_E\}$ as kernel is an isomorphism; an isogeny having the same domain and range is an endomorphism.

Ideal class group The set of all endomorphisms of an elliptic curve E, together with the zero map, form a ring under pointwise addition and composition. Such a ring is called the *endomorphism ring* of E and it is denoted by $\mathrm{End}(E)$. If $\mathrm{End}(E)$ is an order in a quaternion algebra, the curve is said to be *supersingular*, if otherwise it is said to be *ordinary*. The restriction $\mathrm{End}_p(E)$ to the endomorphisms defined over $\mathbb{F}_p$ forms a subring, which is isomorphic to an order in the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{-p})$. An order is a subring of $\mathbb{Q}(\sqrt{-p})$ which is also a finitely-generated $\mathbb{Z}$-module containing a basis of $\mathbb{K}$ as a $\mathbb{Q}$-vector space. The set $\mathbb{Z}[\sqrt{-p}] = \{m + n\sqrt{-p} \mid m, n \in \mathbb{Z}\}$ satisfies the above three conditions, and we will denote it by $\mathcal{O}$. We then consider the set $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ containing all supersingular curves E defined over $\mathbb{F}_p$ - modulo isomorphisms defined over $\mathbb{F}_p$ - such that there exists an isomorphism between $\mathcal{O}$ and $\mathrm{End}_p(E)$ mapping $\sqrt{-p} \in \mathcal{O}$ into the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$. Each isomorphism class in $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ can be uniquely represented by a single element of $\mathbb{F}_p$ if $p \geq 5$ is a prime such that $p \equiv 3 \pmod 8$.

A *fractional ideal* $\mathfrak{a}$ of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule of $\mathbb{K}$. When $\mathfrak{a}$ is contained in $\mathcal{O}$, it is said to be *integral*; when $\mathfrak{a} = \alpha\mathcal{O}$ for some $\alpha \in \mathbb{K}$, it is said to be *principal*; when there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$, it is called *invertible*. The set of invertible fractional ideals of $\mathcal{O}$ forms an abelian group under ideal multiplication. Its quotient by the subgroup composed by principal fractional ideals is a finite group called *ideal class group* of $\mathcal{O}$, usually denoted by $\mathcal{C}\ell(\mathcal{O})$, which cardinality is the class number of $\mathcal{O}$.

The ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on the set $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ via a group action, which denote by $\star$.

$$\begin{aligned} \star : \mathcal{C}\ell(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) &\to \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) \\ (\mathfrak{a}, E) &\mapsto \mathfrak{a} \star E. \end{aligned}$$

For convenience, we use representatives instead of equivalence classes to denote elements of $\mathcal{C}\ell(\mathcal{O})$ and $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$. When p is of the form $4\ell_1\ell_2\cdots\ell_s-1$, where $\ell_1,\ldots,\ell_s$ are small odd primes, a special integral ideal $\mathfrak{J}_{\ell_i}\subset\mathcal{O}$ corresponds to each prime ℓ_i. These ideals allow an efficient computation of the group action. In particular, the action of $\mathfrak{J}_{\ell_i}$ on a curve $E\in\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ is determined by an isogeny having as kernel the unique rational ℓ_i-torsion subgroup of E.

The CSIDH setting [8] The general variant of the CSIDH key-exchange scheme relies on the heuristic that the equivalence classes of the ideals $\mathfrak{J}_{\ell_1},\ldots,\mathfrak{J}_{\ell_s}$, together with their inverses, generate the entire ideal class group $\mathcal{C}\ell(\mathcal{O})$. Castryck et al. proposed a *non-interactive* key exchange with using of supersingular elliptic curves over $\mathbb{F}_p$ with $p\equiv 3 \pmod 3$. It starts from the curve $E_0: y^2=x^3+x$ with $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O}$. As known, all Montgomery curves $E_A: y^2=x^3+Ax^2+x$ over $\mathbb{F}_p$ that are supersingular appear in the $\mathcal{C}\ell(\mathcal{O})$-orbit of E_0, and even their $\mathbb{F}_p$-isomorphism class is uniquely determined by A. It gives the small public key size by a single $\mathbb{F}_p$-element A for checking its supersingularity.

Throughout this paper, we use the following notation: For a positive integer n, let $[n]=\{1,2,\ldots,n\}$. For n values $x_1,\ldots,x_n$, let $(x_i)_{i\in[n]}=(x_1,\ldots,x_n)$. For a function $f:\mathbb{N}\to\mathbb{R}$, f is negligible in λ if $f(\lambda)=o(\lambda^{-c})$ for any constant $c>0$ and sufficiently large $\lambda\in\mathbb{N}$. Then, we write $f(\lambda)=\mathsf{negl}(\lambda)$. A probability is an overwhelming probability if it is $1-\mathsf{negl}(\lambda)$. "Probabilistic polynomial-time" is abbreviated as PPT. For a positive integer λ, let $\mathsf{poly}(\lambda)$ be a universal polynomial of λ.

2.2 Lossy Identification Schemes

Following [1,14], we describe the definition of lossy identification schemes.

Definition 1 (Lossy Identification Scheme). *A lossy identification scheme for a relation $\mathcal{R}\subseteq\mathcal{X}\times\mathcal{Y}$ consists of five polynomial-time algorithms $(\mathsf{IGen},\mathsf{LossyIGen},\mathsf{P}=(\mathsf{P}_1,\mathsf{P}_2),\mathsf{V})$: Let ComSet, ChSet, and ResSet be the commitment space, the challenge space, and the response space, respectively.*

Key Generation. *The randomized algorithm IGen takes as input a security parameter 1^λ and outputs a statement-witness pair $(X,W)\in\mathcal{R}$.*

Lossy Key Generation. *The randomized algorithm $\mathsf{LossyIGen}$ takes as input a security parameter 1^λ and outputs a statement $X_{\mathsf{los}}\in\mathcal{X}$.*

Prover. *The prover protocol P is split into two randomized algorithms $(\mathsf{P}_1,\mathsf{P}_2)$:*

- *The randomized algorithm P_1 takes as input a statement-witness pair (X,W) and outputs a commitment $com\in\mathsf{ComSet}$.*
- *The randomized or deterministic algorithm P_2 takes as input a statement-witness pair $(X,W)\in\mathcal{R}$, a commitment $com\in\mathsf{ComSet}$, and a challenge $ch\in\mathsf{ChSet}$, and it outputs a response $resp\in\mathsf{ResSet}$.*

Verifier. *The deterministic algorithm V takes as input a statement X, a commitment $com\in\mathsf{ComSet}$, a challenge $ch\in\mathsf{ChSet}$, and a response $resp\in\mathsf{ResSet}$, and it outputs 1 (accept) or 0 (reject).*

In addition, following [1], we describe the transcript generation protocol $\mathsf{Trans}_{X,W}^{\mathsf{LossyID}}$ for a lossy identification scheme $(\mathsf{IGen},\mathsf{LossyIGen},\mathsf{P}=(\mathsf{P}_1,\mathsf{P}_2),\mathsf{V})$. For every $(X,W)\leftarrow\mathsf{IGen}(\lambda)$, $\mathsf{Trans}_{X,W}^{\mathsf{LossyID}}()$ generates a transcript $(com,ch,resp)\in\mathsf{ComSet}\times\mathsf{ChSet}\times\mathsf{ResSet}\cup\{(\bot,\bot,\bot)\}$, in the following way:

1. Compute $com\leftarrow\mathsf{P}_1(X,W)$.
2. Choose $ch\xleftarrow{\$}\mathsf{ChSet}$.
3. Compute $resp\leftarrow\mathsf{P}_2((X,W),com,ch)$.
4. If $resp=\bot$, set $(com,ch)\leftarrow(\bot,\bot)$.
5. Output $(com,ch,resp)$.

The required properties for a lossy identification scheme are as follows:

Definition 2. *A lossy identification scheme $\mathsf{LossyID}=(\mathsf{IGen},\mathsf{LossyIGen},\mathsf{P}=(\mathsf{P}_1,\mathsf{P}_2),\mathsf{V})$ is required to satisfy the following properties:*

Completeness. *For every* $(X, W) \leftarrow \mathsf{IGen}(1^\lambda)$*, it holds that*

$$\Pr\left[\mathsf{V}(X, com, ch, resp) = 1 \;\middle|\; \begin{array}{c} com \leftarrow \mathsf{P}_1(X, W); ch \xleftarrow{\$} \mathsf{ChSet}; \\ resp \leftarrow \mathsf{P}_2(X, W, com, ch) \end{array}\right] = 1.$$

Honest-Verifier Zero-Knowledge. *For every* $(X, W) \leftarrow \mathsf{IGen}(1^\lambda)$*, there exists a PPT simulator* Sim *which, on input a statement* X*, outputs transcripts* $\{(com, ch, resp)\}$ *whose distributions are statistically indistinguishable from those of the transcripts generated by* $\mathsf{Trans}^{\mathsf{LossyID}}_{X,W,\lambda}$.

Indistinguishability of Lossy Statements. *For any PPT adversary* $\mathcal{A}$ *against* IDS*, its advantage*

$$\mathsf{Adv}^{\text{ind-stmt}}_{\mathsf{IDS},\mathcal{A}}(\lambda) := \left|\Pr[\mathcal{A}(X) = 1 \mid (X, W) \leftarrow \mathsf{IGen}(1^\lambda)] - \Pr[\mathcal{A}(X_{\mathsf{los}}) = 1 \mid X_{\mathsf{los}} \leftarrow \mathsf{LossyIGen}(1^\lambda)]\right|$$

is negligible in λ.

Lossy Soundness. $\mathsf{LossyID}$ *satisfies* ϵ_{los}*-lossy soundness if for any unbounded adversary* $\mathcal{A}$ *against* $\mathsf{LossyID}$*, its advantage* $\mathsf{Adv}^{\text{los-imp-pa}}_{\mathsf{LossyID},\mathcal{A}}(\lambda) = \Pr[\mathsf{Expt}^{\text{los-imp-pa}}_{\mathsf{LossyID},\mathcal{A}}(\lambda) = 1]$ *is less than* ϵ_{los}*, where* $\mathsf{Expt}^{\text{los-imp-pa}}_{\mathsf{LossyID},\mathcal{A}}(\lambda)$ *is the following experiment:*

1. *A challenger generates* $X_{\mathsf{los}} \leftarrow \mathsf{LossyIGen}(1^\lambda)$ *and gives* X_{los} *to the adversary* $\mathcal{A}$.
2. $\mathcal{A}$ *submits a commitment* $com \in \mathsf{ComSet}$ *to the challenger. The challenger returns a challenge* $ch \xleftarrow{\$} \mathsf{ChSet}$.
3. $\mathcal{A}$ *outputs a response* $resp \in \mathsf{ResSet}$*. The challenger returns* $b \leftarrow \mathsf{V}(X_{\mathsf{los}}, com, ch, resp)$.

2.3 Identity-based Signatures

Following [17,30], we describe the syntax and a security definition for identity-based signatures (IBSs), as follows:

Definition 3 (IBS). *An IBS scheme consists of polynomial-time algorithms* $(\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vrfy})$*: For a security parameter* λ*, let* $\mathcal{ID} = \mathcal{ID}(\lambda)$ *be the identity space, let* $\mathcal{M} = \mathcal{M}(\lambda)$ *be the message space, and let* $\mathcal{USK} = \mathcal{USK}(\lambda)$ *be the user secret key space.*

Setup. *The randomized algorithm* Setup *takes as input a security parameter* 1^λ *and outputs a master public key* mpk *and a master secret key* msk.

Key Derivation. *The randomized algorithm* KeyDer *takes as input a master public key* mpk*, a master secret key* msk*, and an identity* id*, and it outputs a user secret key* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$.

Signing. *The randomized or deterministic algorithm* Sign *takes as input a master public key* mpk*, a user secret key* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, and a message* $\mathsf{m} \in \mathcal{M}$*, and it outputs a signature* σ.

Verification. *The deterministic algorithm* Vrfy *takes as input a master public key* mpk*, an identity* $\mathsf{id} \in \mathcal{ID}$*, a message* $\mathsf{m} \in \mathcal{M}$*, and a signature* σ*, and it outputs* 1 *(accept) or* 0 *(reject).*

We require an IBS scheme to be *correct*, as follows:

Definition 4 (Correctness). *An IBI scheme* $(\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vrfy})$ *is* correct*, if for every* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$*, every* $\mathsf{id} \in \mathcal{ID}$*, and every* $\mathsf{m} \in \mathcal{M}$*, it holds that* $\mathsf{Vrfy}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) = 1$*, where* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ *and* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}[\mathsf{id}], \mathsf{m})$.

As a security notion of IBSs, we describe the definition of *existential unforgeability against chosen identity and chosen message attacks* (called $\mathsf{EUF\text{-}ID\text{-}CMA}$ security) [30].

Definition 5 ($\mathsf{EUF\text{-}ID\text{-}CMA}$ security). *An IBS scheme* $\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vrfy})$ *is* $\mathsf{EUF\text{-}ID\text{-}CMA}$ *secure, if for any PPT adversary* $\mathcal{A}$ *against* IBS*, its advantage* $\mathsf{Adv}^{\text{euf-id-cma}}_{\mathsf{IBS},\mathcal{A}}(\lambda) := \Pr[\mathsf{Expt}^{\text{euf-id-cma}}_{\mathsf{IBS},\mathcal{A}}(\lambda) = 1]$ *is negligible in* λ*, where the experiment* $\mathsf{Expt}^{\text{euf-id-cma}}_{\mathsf{IBS},\mathcal{A}}(\lambda)$ *is defined as follows:*

Setup. *The challenger generates* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and sets the four lists* $\mathcal{L}_{\mathsf{id}} \leftarrow \emptyset$*,* $\hat{\mathcal{L}}_{\mathsf{id}} \leftarrow \emptyset$*,* $\mathcal{L}_{\mathsf{usk}_{\mathsf{id}}} \leftarrow \emptyset$*, and* $\mathcal{L}_{\mathsf{m}} \leftarrow \emptyset$*. It gives* mpk *to the adversary* $\mathcal{A}$.

Queries. $\mathcal{A}$ *is given access to the following oracles:*

- *Key derivation oracle* $\mathsf{O}_{\mathsf{KeyDer}}$*: On input a key derivation query* $\mathsf{id} \in \mathcal{ID}$*,* $\mathsf{O}_{\mathsf{KeyDer}}$ *outputs* $\perp$ *if* $\mathsf{id} \in \hat{\mathcal{L}}_{\mathsf{id}}$*. Then, it checks whether* $(\mathsf{id}, \cdot) \in \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}}$*. If* $(\mathsf{id}, \mathsf{usk}_{\mathsf{id}}) \in \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}}$ *for some* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, it returns* $\mathsf{usk}_{\mathsf{id}}$*. Otherwise, it returns* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ *and sets the two lists* $\mathcal{L}_{\mathsf{usk}_{\mathsf{id}}} \leftarrow \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}} \cup \{(\mathsf{id}, \mathsf{usk}_{\mathsf{id}})\}$*,* $\mathcal{L}_{\mathsf{id}} \leftarrow \mathcal{L}_{\mathsf{id}} \cup \{\mathsf{id}\}$*.*
- *Signing oracle* $\mathsf{O}_{\mathsf{Sign}}$*: On input a signing-query* $(\mathsf{id}, \mathsf{m}) \in \mathcal{ID} \times \mathcal{M}$*,* $\mathsf{O}_{\mathsf{Sign}}$ *sets* $\mathcal{L}_{\mathsf{m}} \leftarrow \mathcal{L}_{\mathsf{m}} \cup \{(\mathsf{id}, \mathsf{m})\}$ *and checks whether* $(\mathsf{id}, \mathsf{usk}_{\mathsf{id}}) \in \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}}$*:*
  - *If* $(\mathsf{id}, \mathsf{usk}_{\mathsf{id}}) \in \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}}$ *for some* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, it returns* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{m})$*.*
  - *If there does not exist* $(\mathsf{id}, \mathsf{usk}_{\mathsf{id}}) \in \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}}$ *such that* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, it computes* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$*, sets* $\mathcal{L}_{\mathsf{usk}_{\mathsf{id}}} \leftarrow \mathcal{L}_{\mathsf{usk}_{\mathsf{id}}} \cup \{(\mathsf{id}, \mathsf{usk}_{\mathsf{id}})\}$*,* $\hat{\mathcal{L}}_{\mathsf{id}} \leftarrow \hat{\mathcal{L}}_{\mathsf{id}} \cup \{\mathsf{id}\}$*, and returns* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{m})$*.*

Output. $\mathcal{A}$ *outputs a forgery* $(\mathsf{id}^*, \mathsf{m}^*, \sigma^*)$*. The challenger outputs* 1 *if* $\mathsf{id}^* \notin \mathcal{L}_{\mathsf{id}} \wedge (\mathsf{id}^*, \mathsf{m}^*) \notin \mathcal{L}_{\mathsf{m}} \wedge \mathsf{Vrfy}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{m}^*, \sigma^*) = 1$*, and* 0 *otherwise.*

2.4 Hardness Assumptions

We describe the definitions of the computational assumptions related to our IBS scheme's security: The *decisional CSIDH* and *fixed-curve multi-decisional CSIDH* assumptions.

Following [14], we describe the decisional CSIDH (D-CSIDH) and fixed-curve multi-decisional CSIDH (FCMD-CSIDH) assumptions, as follows:

Definition 6 (Decisional CSIDH Assumption). *Given the set* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ *and the ideal class group* $\mathcal{C}\ell(\mathcal{O})$*, the decisional CSIDH (*D-CSIDH*) problem is to distinguish between the following distributions:*

- $(E, H, \mathfrak{a} \star E, \mathfrak{a} \star H)$*, where the supersingular elliptic curves* E *and* H *are sampled uniformly from* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$*, and* $\mathfrak{a}$ *is sampled uniformly from* $\mathcal{C}\ell(\mathcal{O})$*,*
- (E, H, E', H')*, where* E, H, E', H' *are supersingular elliptic curves sampled uniformly from* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$*.*

We say that the D-CSIDH *assumption holds if for any PPT algorithm* $\mathcal{A}$*, its advantage* $\mathsf{Adv}^{\mathsf{D\text{-}CSIDH}}_{\mathcal{A}}(\lambda)$ *is negligible in* λ*, where* $\mathsf{Adv}^{\mathsf{D\text{-}CSIDH}}_{\mathcal{A}}(\lambda)$ *is the advantage of* $\mathcal{A}$ *distinguishing the above two distributions.*

Definition 7 (Fixed-Curve Multi-Decisional CSIDH Assumption). *Let* S *be a positive integer. Given the ideal class group* $\mathcal{C}\ell(\mathcal{O})$ *and the set* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$*, the fixed-curve multi-decisional CSIDH (*FCMD-CSIDH*) problem with* S *is to distinguish the following distributions:*

- $(E, H, (\mathfrak{a}_i \star E, \mathfrak{a}_i \star H)_{i \in [S]})$*, where the supersingular elliptic curves* E *and* H *are sampled uniformly from* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$*, and for* $i \in [S]$*,* $\mathfrak{a}_i$ *are sampled uniformly from* $\mathcal{C}\ell(\mathcal{O})$*,*
- $(E, H, (E'_i, H'_i)_{i \in [S]})$*, where* E, H, E'_i, H'_i *for* $i \in [S]$ *are supersingular elliptic curves sampled from* $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ *uniformly at random.*

We say that the FCMD-CSIDH *assumption with parameter* S *holds if for any PPT algorithm* $\mathcal{A}$*, its advantage* $\mathsf{Adv}^{\mathsf{FCMD\text{-}CSIDH}}_{\mathcal{A},S}(\lambda)$ *is negligible in* λ*, where* $\mathsf{Adv}^{\mathsf{FCMD\text{-}CSIDH}}_{\mathcal{A},S}(\lambda)$ *is the advantage of* $\mathcal{A}$ *distinguishing the above two distributions.*

From a result of [14], the following relationship between the above two assumptions was shown:

Lemma 1 (D-CSIDH to FCMD-CSIDH ([14])). *Let* S *be a positive integer. If there exists any PPT algorithm* $\mathcal{A}$ *solving the* FCMD-CSIDH *problem with parameter* S*, then there exists a PPT algorithm* $\mathcal{B}$ *solving the* D-CSIDH *problem such that*

$$\mathsf{Adv}^{\mathsf{FCMD\text{-}CSIDH}}_{\mathcal{A},S}(\lambda) \leq S \cdot \mathsf{Adv}^{\mathsf{D\text{-}CSIDH}}_{\mathcal{B}}(\lambda).$$

3 The Lossy CFI-FiSh scheme

In this section, we first recall the construction of the lossy CFI-FiSh identification scheme [14].

3.1 The lossy CFI-FiSh

The lossy CFI-FiSh identification scheme $(\mathsf{IGen}, \mathsf{LossyIGen}, \mathsf{P}_1, \mathsf{P}_2, \mathsf{V})$ is constructed as follows:

The following system parameter of the lossy CSI-FiSh is set: Assume the ideal class group $\mathcal{C}\ell(\mathcal{O})$ is cyclic with a known order N and generator $\mathfrak{g}$. Let E_0 be the base curve defined by $y^2 = x^3 + x$. Let $\mathcal{X}$ be a finite set of pairs $((E_1^{(0)}, E_2^{(0)}), (E_1^{(1)}, E_2^{(1)}))$ where $E_1^{(0)}, E_2^{(0)}, E_1^{(1)}, E_2^{(1)}$ are being run over $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$. Here, $\mathcal{Y} = \mathbb{Z}_N$ is the set of witnesses. Consider the relation

$$\mathcal{R} := \{(((E_1^{(0)}, E_2^{(0)}), (E_1^{(1)}, E_2^{(1)})), a) \in \mathcal{X} \times \mathcal{Y} \mid E_1^{(1)} = \mathfrak{g}^a \star E_1^{(0)}, E_2^{(1)} = \mathfrak{g}^a \star E_2^{(0)}\},$$

where $((E_1^{(0)}, E_2^{(0)}), (E_1^{(1)}, E_2^{(1)})) \in \mathcal{X}$ is a statement, and $a \in \mathcal{Y}$ is a witness.

- The IGen algorithm samples $a, b, c \in \mathbb{Z}_N$ uniformly at random and outputs a pair $(X, W) \in \mathcal{R}$ where $X = ((E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0), (E_1^{(1)} = \mathfrak{g}^a \star E_1^{(0)}, E_2^{(1)} = \mathfrak{g}^a \star E_2^{(0)}))$ and $W = a$
- The $\mathsf{LossyIGen}$ algorithm chooses $a, a', b, c \in \mathbb{Z}_N$ uniformly at random and outputs a lossy statement $X_{ls} = ((E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0), (E_1^{(1)} = \mathfrak{g}^a \star E_1^{(0)}, E_2^{(1)} = \mathfrak{g}^{a'} \star E_2^{(0)}))$
- The P_1 algorithm takes (X, W) as input and generates a uniformly random $r \in \mathbb{Z}_N$. This algorithm outputs the commitment $com = (F_1 = \mathfrak{g}^r \star E_1^{(0)}, F_2 = \mathfrak{g}^r \star E_2^{(0)})$.
- The P_2 algorithm, on input $((X, W), com, ch)$ where $ch \in \{0, 1\}$, outputs the response $resp = r$ if $ch = 0$, else $resp = r - a$.
- The V algorithm given $(X, com, ch, resp)$ accepts if the following equations hold:

$$\begin{cases} \mathfrak{g}^{resp} \star E_1^{(0)} = F_1, \mathfrak{g}^{resp} \star E_2^{(0)} = F_2, & \text{if } ch = 0 \\ \mathfrak{g}^{resp} \star E_1^{(1)} = F_1, \mathfrak{g}^{resp} \star E_2^{(1)} = F_2, & \text{if } ch = 1 \end{cases}$$

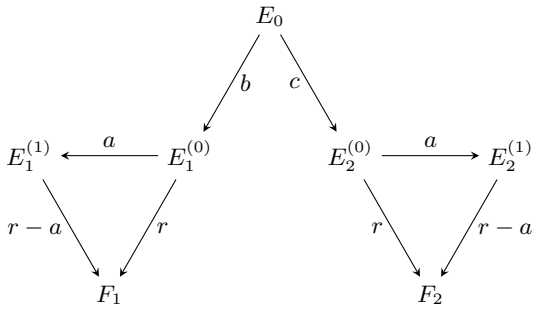

Fig. 1. The base lossy CFI-FiSh identification scheme in[14]

From results of [14], the following proposition was proved:

Proposition 1 ([14]). *The lossy identification scheme* $\mathsf{LossyID}^{\mathsf{base}}$ *satisfies* completeness *and* honest-verifier zero-knowledge *property.*

- $\mathsf{LossyID}^{\mathsf{base}}$ *satisfies* indistinguishability of lossy statements *if the* D-CSIDH *assumption holds. In particular, we have* $\mathsf{Adv}^{\text{ind-stmt}}_{\mathcal{A},\mathsf{LossyID}^{\mathsf{base}}}(\lambda) = \mathsf{Adv}^{\mathsf{D\text{-}CSIDH}}_{\mathcal{B}}(\lambda)$*, where* $\mathcal{A}$ *is a PPT algorithm against* $\mathsf{LossyID}^{\mathsf{base}}$*, and* $\mathcal{B}$ *is a PPT algorithm against the* D-CSIDH *problem.*
- $\mathsf{LossyID}^{\mathsf{base}}$ *satisfies* ϵ_{los}-lossy soundness *for* $\epsilon_{\mathsf{los}} = 1/(2N)$*, where* $N = |\mathcal{C}\ell(\mathcal{O})|$.

The above lossy identification scheme has only one-bit challenge. To improve the security, we need to execute the base lossy identification scheme in parallel rounds. To decrease the signature size of the resulting Fiat-Shamir signature scheme, a method in [12] is applied which need to satisfy the size of public key. The concrete construction is as follows: As the security parameter, let $\mathbf{X} = \{(E_1^{(0)}, E_2^{(0)}), (E_1^{(1)}, E_2^{(1)}), \cdots, (E_1^{(S)}, E_2^{(S)}) \mid E_i^{(j)} \in \mathcal{E}\ell\ell_p(\mathcal{O})\}, Y = \{a_1, a_2, \cdots, a_S | a_i \in \mathbb{Z}_N\}$. E_0 is defined the same as the base lossy CFI-FiSh.

- The algorithm IGen takes $\{a_i\}_{i\in[S]}, b, c \in \mathbb{Z}_N$ and outputs a pair $(X, W) \in \mathcal{R}$ where $X = ((E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0), (E_1^{(1)} = \mathfrak{g}^{a_1} \star E_1^{(0)}, E_2^{(i)} = \mathfrak{g}^{a_1} \star E_2^{(0)}), \cdots, (E_1^{(S)} = \mathfrak{g}^{a_S} \star E_1^{(0)}, E_2^{(S)} = \mathfrak{g}^{a_S} * E_2^{(0)}))$ and $W = \{a\}_i$

- The algorithm $\mathsf{LossyIGen}$ takes $a_1, a_2, \cdots, a_S, a'_1, a'_2, \cdots, a'_S, b, c \in \mathbb{Z}_N$ and outputs a lossy statement $X_{ls} = ((E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0), (E_1^{(1)} = \mathfrak{g}^{a_1} \star E_1^{(0)}, E_2^{(1)} = \mathfrak{g}^{a'_1} \star E_2^{(0)}), \cdots, (E_1^{(S)} = \mathfrak{g}^{a_S} \star E_1^{(0)}, E_2^{(S)} = \mathfrak{g}^{a'_S} \star E_2^{(0)}))$

- P_1 takes the output (X, W) of the algorithm IGen and then generates t random $r_i \in \mathbb{Z}_N$. The output of P_1 is the commitment $com = (F_1^{(i)} = \mathfrak{g}^r \star E_1^{(0)}, F_2^{(i)} = \mathfrak{g}^r \star E_2^{(0)})$

- P_2 takes $((X, W), com, ch)$ where $ch = b_1||b_2||\cdots||b_t$, each $b_i \in \{0, 1, \cdots, S\}$ and outputs the response $resp = resp_1||resp_2||\cdots||resp_t$, $resp_i = r_i$ if $b_i = 0$, else $resp_i = r_i - a_i$.

- The algorithm V takes $(X, com, ch, resp)$ and accepts if the following equations hold

$$\begin{cases} \mathfrak{g}^{resp_i} \star E_1^{(0)} = F_1, \mathfrak{g}^{resp_i} \star E_2^{(0)} = F_2, & \text{if } b_i = 0 \\ \mathfrak{g}^{resp} \star E_1^{(1)} = F_1, \mathfrak{g}^{resp} \star E_2^{(1)} = F_2, & \text{if } b_i \neq 0 \end{cases}$$

4 Tightly Secure IBS from Lossy CSI-FiSh

4.1 Construction

In this section, we describe our proposed IBS scheme with tight security. This scheme is based on the lossy CSI-FiSh scheme and IBS scheme in [27]. Informally, our IBS is described as follows:

- The master public key mpk and the master secret key msk are a public key $(E_1^{(i)}, E_2^{(i)})_{i\in\{0,\ldots,S_0\}}$ and a secret key $(a_i)_{i\in[S_0]}$ of the lossy CSI-FiSh scheme, respectively.
- When generating a user's secret key $\mathsf{usk}_{\mathsf{id}}$, a lossy CSI-FiSh's signature $(F_1^{(i,j)}, F_2^{(i,j)}, resp_{i,j})_{i\in[T_1],j\in[S_1]}$ on id is generated by using msk. Then, this signature corresponds to $\mathsf{usk}_{\mathsf{id}}$ in our scheme.
- The Sign algorithm on input $\mathsf{usk}_{\mathsf{id}}$ and a message m generates a signature on $(\mathsf{id}, \mathsf{m})$, which consists of the commitment $(F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}$ and a new lossy CSI-FiSh's signature $(\widehat{ch}_{i,j}, \widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]}$ computed by using $\mathsf{usk}_{\mathsf{id}}$.
- The Vrfy algorithm checks the validity-check of the given signature on $(\mathsf{id}, \mathsf{m})$, by following the verification algorithm of the lossy CSI-FiSh scheme.

Concretely, our proposed IBS scheme $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vrfy})$ is constructed as follows: As the system parameter of $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$, let E_0 be the base curve, let $T_1, T_2, S_0 = 2^{\eta_0} - 1, S_1 = 2^{\eta_1} - 1$ be positive integers, where η_0, η_1 are positive integers, and $T_1 < S_0, T_2 < S_1$. Let $H : \{0,1\}^* \to \{0, \ldots, S_0\}^{T_1 S_1}$ and $\hat{H} : \{0,1\}^* \to \{0, \ldots, S_1\}^{T_1 T_2}$ be random oracles. $\mathcal{ID} = \{0,1\}^*$ and $\mathcal{M} = \{0,1\}^*$ are the identity space and the message space, respectively.

- $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$:
  1. Choose $b \xleftarrow{\$} \mathbb{Z}_N$ and $c \xleftarrow{\$} \mathbb{Z}_N$.
  2. Compute $E_1^{(0)} = \mathfrak{g}^b \star E_0$ and $E_2^{(0)} = \mathfrak{g}^c \star E_0$.
  3. For $i \in \{1, \ldots, S_0\}$, choose $a_i \xleftarrow{\$} \mathbb{Z}_N$ and compute $E_1^{(i)} = \mathfrak{g}^{a_i} \star E_1^{(0)}$, $E_2^{(i)} = \mathfrak{g}^{a_i} \star E_2^{(0)}$.
  4. Output $\mathsf{mpk} = ((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)}, E_2^{(i)})_{i\in[S_0]})$ and $\mathsf{msk} = (a_1, \ldots, a_{S_0})$.
- $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  1. Parse $((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)}, E_2^{(i)})_{i\in[S_0]})$ and $\mathsf{msk} = (a_1, \ldots, a_{S_0})$.
  2. For $i \in [T_1]$ and $j \in [S_1]$, choose $r_{i,j} \xleftarrow{\$} \mathbb{Z}_N$ and compute $F_1^{(i,j)} = \mathfrak{g}^{r_{i,j}} \star E_1^{(0)}$, $F_2^{(i,j)} = \mathfrak{g}^{r_{i,j}} \star E_2^{(0)}$.
  3. Compute $(ch_i)_{i\in[T_1 S_1]} = H((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]} \parallel \mathsf{id})$.
  4. For $i \in [T_1]$ and $j \in [S_1]$, compute $resp_{i,j} = r_{i,j} - a_{ch_i}$.

5. Output $\mathsf{usk}_{\mathsf{id}} = (\mathsf{id}, (F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (resp_{i,j})_{i\in[T_1],j\in[S_1]})$.

– $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{m})$:

1. Parse $\mathsf{mpk} = ((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)}, E_2^{(i)})_{i\in[S_0]})$ and $\mathsf{usk}_{\mathsf{id}} = (\mathsf{id}, (F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (resp_{i,j})_{i\in[T_1],j\in[S_1]})$.
2. For $i \in [T_1]$, set $resp_{i,0} = 0$.
3. Compute $(ch_i)_{i\in[T_1S_1]} = H((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]} \parallel \mathsf{id})$.
4. For $i \in [T_1]$ and $j \in [T_2]$, choose $\hat{r}_{i,j} \xleftarrow{\$} \mathbb{Z}_N$ and compute $\hat{F}_1^{(i,j)} = \mathfrak{g}^{\hat{r}_{i,j}} \star E_1^{(ch_i)}$, $\hat{F}_2^{(i,j)} = \mathfrak{g}^{\hat{r}_{i,j}} \star E_2^{(ch_i)}$.
5. Compute $(\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]} = \hat{H}((\hat{F}_1^{(i,j)}, \hat{F}_2^{(i,j)})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m})$.
6. For $i \in [T_1]$ and $j \in [T_2]$, compute $\widehat{resp}_{i,j} = \hat{r}_{i,j} - resp_{i,\widehat{ch}_{i,j}}$.
7. Output $\sigma = ((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]})$.

– $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma)$:

1. Parse $\mathsf{mpk} = ((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)}, E_2^{(i)})_{i\in[S_0]})$ and $\sigma = ((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]})$.
2. Compute $(ch_i)_{i\in[T_1S_1]} = H((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]} \parallel \mathsf{id})$.
3. For $i \in [T_1]$ and $j \in [T_2]$, compute
   - $\hat{F}_1^{(i,j)\prime} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_1^{(ch_i)}$ and $\hat{F}_2^{(i,j)\prime} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_2^{(ch_i)}$ if $\widehat{ch}_{i,j} = 0$, and
   - $\hat{F}_1^{(i,j)\prime} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_1^{(i,\widehat{ch}_{i,j})}$ and $\hat{F}_2^{(i,j)\prime} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_2^{(i,\widehat{ch}_{i,j})}$ if $\widehat{ch}_{i,j} > 0$.
4. Output 1 if $(\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]} = \hat{H}((\hat{F}_1^{(i,j)\prime}, \hat{F}_2^{(i,j)\prime})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m})$, and 0 otherwise.

We show the correctness of our scheme $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$, as follows:

Proposition 2. *The IBS scheme* $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$ *is* correct.

Proof. Let $\mathsf{mpk} = ((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)}, E_2^{(i)})_{i\in[S_0]})$ and $\mathsf{msk} = (a_1, \ldots, a_{S_0})$, where $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$. For an identity $\mathsf{id} \in \mathcal{ID}$ and a message $\mathsf{m} \in \mathcal{M}$, let $\mathsf{usk}_{\mathsf{id}} = (\mathsf{id}, (F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (resp_{i,j})_{i\in[T_1],j\in[S_1]}) \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ and let $\sigma = ((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]}) \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{m})$.

Then, we show that the verification algorithm Vrfy accepts the valid message-signature pair (m, σ) on id.

In the case $\widehat{ch}_{i,j} = 0$, for $(i,j) \in [T_1] \times [T_2]$ and $k \in \{1,2\}$, we have

$$\begin{aligned}\hat{F}_k^{(i,j)\prime} &= \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_k^{(ch_i)} \\ &= \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,\widehat{ch}_{i,j}}} \star E_k^{(ch_i)} \\ &= \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,0}} \star E_k^{(ch_i)} \\ &= \mathfrak{g}^{\hat{r}_{i,j}} \star E_k^{(ch_i)} = \hat{F}_k^{(i,j)}.\end{aligned}$$

In the case $\widehat{ch}_{i,j} > 0$, we have the following for $(i,j) \in [T_1] \times [T_2]$ and $k \in \{1,2\}$:

$$\begin{aligned}\hat{F}_k^{(i,j)\prime} &= \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_k^{(i,\widehat{ch}_{i,j})} \\ &= \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,\widehat{ch}_{i,j}}} \star (\mathfrak{g}^{r_{i,\widehat{ch}_{i,j}}} \star E_k^{(0)}) \\ &= \mathfrak{g}^{\hat{r}_{i,j} - (r_{i,\widehat{ch}_{i,j}} - a_{ch_i})} \star (\mathfrak{g}^{r_{i,\widehat{ch}_{i,j}}} \star E_k^{(0)}) \\ &= \mathfrak{g}^{\hat{r}_{i,j}} \star (\mathfrak{g}^{a_{ch_i}} \star E_k^{(0)}) \\ &= \mathfrak{g}^{\hat{r}_{i,j}} \star E_k^{(ch_i)} = \hat{F}_k^{(i,j)}.\end{aligned}$$

From the above, we obtain the following equation:

$$\begin{aligned}(\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]} &= \hat{H}((\hat{F}_1^{(i,j)}, \hat{F}_2^{(i,j)})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m}) \\ &= \hat{H}((\hat{F}_1^{(i,j)\prime}, \hat{F}_2^{(i,j)\prime})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m}).\end{aligned}$$

Therefore, if a signature σ on an identity-message pair $(\mathsf{id}, \mathsf{m})$ is generated correctly, the Vrfy algorithm accepts this signature. The proof is completed. □

4.2 Security Analysis

The following theorem shows the security of our proposed IBS scheme $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$:

Theorem 1. *If the* FCMD-CSIDH *assumption with parameter S_0 holds, then the IBS scheme* $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$ *is* EUF-ID-CMA *secure in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary against the EUF-ID-CMA security of $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$. Let q_s, q_k, q_h, and $q_{\hat{h}}$ be the maximum numbers of queries issued to the oracles $\mathsf{O}_{\mathsf{Sign}}$, $\mathsf{O}_{\mathsf{KeyDer}}$, H, and $\hat{H}$, respectively.

In order to prove Theorem 1, we consider a sequence of the security games $\mathsf{Game}_0, \mathsf{Game}_1, \mathsf{Game}_2, \mathsf{Game}_3$. For $i \in \{0,1,2,3\}$, let W_i be the event that the experiment outputs 1 in Game_i.

$\underline{\mathsf{Game}_0}$: This game is the same as the ordinary EUF-ID-CMA security game. Then, we have $\mathsf{Adv}^{\text{euf-id-cma}}_{\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}},\mathcal{A}}(\lambda) = \Pr[W_0]$.

$\underline{\mathsf{Game}_1}$: This game is the same as Game_0 except that the key-derivation oracle $\mathsf{O}_{\mathsf{KeyDer}}$ generates a user secret key $\mathsf{usk}_{\mathsf{id}}$ for $\mathsf{id} \in \mathcal{ID}$, as follows:

1. For $i \in [T_1 S_1]$, choose $ch_i \xleftarrow{\$} \{0, \ldots, S_0\}$.
2. For $i \in [T_1]$, set $resp_{i,0} = 0$.
3. For $i \in [T_1]$ and $j \in [S_1]$, choose $resp_{i,j} \xleftarrow{\$} \mathbb{Z}_N$.
4. For $i \in [T_1]$ and $j \in [S_1]$, compute $F_1^{(i,j)} = \mathfrak{g}^{resp_{i,j}} \star E_1^{(ch_i)}$ and $F_2^{(i,j)} = \mathfrak{g}^{resp_{i,j}} \star E_2^{(ch_i)}$.
5. Program $(ch_i)_{i \in [T_1 S_1]} = H((F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]} \parallel \mathsf{id})$ if the hash value of $((F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]} \parallel \mathsf{id})$ is not defined. Otherwise abort.
6. Let $\mathsf{usk}_{\mathsf{id}} = (\mathsf{id}, (F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]}, (resp_{i,j})_{i \in [T_1], j \in [S_1]})$.

First, we show that the $\mathsf{O}_{\mathsf{KeyDer}}$ oracle is correctly simulated in Game_1 unless the aborting event occurs. Let $\sigma = ((F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]}, (\widehat{ch}_{i,j})_{i \in [T_1], j \in [T_2]}, (\widehat{resp}_{i,j})_{i \in [T_1], j \in [T_2]}) \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{m})$ be a signature generated in Game_1. We analyze the output of the Vrfy algorithm. In the case $\widehat{ch}_{i,j} = 0$, Vrfy computes the following for $(i,j) \in [T_1] \times [T_2]$ and $k \in \{1,2\}$:

$$\begin{aligned}\hat{F}_k^{(i,j)\prime} &= \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_k^{(ch_i)} = \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,\widehat{ch}_{i,j}}} \star E_k^{(ch_i)} \\ &= \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,0}} \star E_k^{(ch_i)} = \mathfrak{g}^{\hat{r}_{i,j}} \star E_k^{(ch_i)} = \hat{F}_k^{(i,j)}.\end{aligned}$$

In the case $\widehat{ch}_{i,j} > 0$, for $(i,j) \in [T_1] \times [T_2]$ and $k \in \{1,2\}$, Vrfy computes the following for a valid signature:

$$\begin{aligned}\hat{F}_k^{(i,j)\prime} &= \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_k^{(i,\widehat{ch}_{i,j})} \\ &= \mathfrak{g}^{\hat{r}_{i,j} - resp_{i,\widehat{ch}_{i,j}}} \star (\mathfrak{g}^{resp_{i,\widehat{ch}_{i,j}}} \star E_k^{(ch_i)}) \\ &= \mathfrak{g}^{\hat{r}_{i,j}} \star E_k^{(ch_i)} = \hat{F}_k^{(i,j)}.\end{aligned}$$

The second equation holds because for any $\widehat{ch}_{i,j} = \tilde{j} > 0$, the $\mathsf{O}_{\mathsf{KeyDer}}$ oracle sets $F_k^{(i,\tilde{j})} = \mathfrak{g}^{resp_{i,\tilde{j}}} \star E_k^{(ch_i)}$.

We next estimate the upper bound of the probability that the $\mathsf{O}_{\mathsf{KeyDer}}$ oracle aborts, that is, the probability that $((F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]} \parallel \mathsf{id})$ has been queried to H when defining $H((F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]} \parallel \mathsf{id})$.

As the worst-case scenario, $q_h + 1$ queries are issued to H at the beginning of the experiment. Then, the probability that $\mathsf{O}_{\mathsf{KeyDer}}$ aborts for the i-th query is at most $(i + q_h)/N$. In addition, the total number of queries issued to H is at most $q_s + q_k$, since $\mathsf{O}_{\mathsf{Sign}}$ and $\mathsf{O}_{\mathsf{KeyDer}}$ call H at most q_s and q_h times, respectively. The probability of guessing a collision of H each time is at most $(q_s + q_k + q_h + 1)/N$. Hence, the probability of aborting Game_1 is at most $(q_s + q_k)(q_s + q_k + q_h + 1)/N$ over all $(q_s + q_k)$ extraction queries, and we have $|\Pr[W_0] - \Pr[W_1]| \leq (q_s + q_k)(q_s + q_k + q_h + 1)/N$.

$\underline{\mathsf{Game}_2}$: This game is the same as Game_1 except that the signing oracle $\mathsf{O}_{\mathsf{Sign}}$ generates a signature σ on $\underline{(\mathsf{id}, \mathsf{m})}$, as follows:

1. Parse $\mathsf{usk}_{\mathsf{id}} = (\mathsf{id}, (F_1^{(i,j)}, F_2^{(i,j)})_{i \in [T_1], j \in [S_1]}, (resp_{i,j})_{i \in [T_1], j \in [S_1]})$.

2. Compute
   $(ch_i)_{i\in[T_1S_1]} = H((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]} \parallel \mathsf{id})$.
3. For $i \in [T_1]$ and $j \in [T_2]$, choose $\widehat{ch}_{i,j} \xleftarrow{\$} \{0,\ldots,S_1\}$ and $\widehat{resp}_{i,j} \xleftarrow{\$} \mathbb{Z}_N$.
4. For $i \in [T_1]$ and $j \in [T_2]$, compute
   - $\hat{F}_1^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_1^{(ch_i)}$ and $\hat{F}_2^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_2^{(ch_i)}$ if $\widehat{ch}_{i,j} = 0$, and
   - $\hat{F}_1^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_1^{(i,\widehat{ch}_{i,j})}$ and $\hat{F}_2^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_2^{(i,\widehat{ch}_{i,j})}$ if $\widehat{ch}_{i,j} > 0$.
5. Program $(\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]} = \hat{H}((\hat{F}_1^{(i,j)}, \hat{F}_2^{(i,j)})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m})$ if the hash value of $((\hat{F}_1^{(i,j)}, \hat{F}_2^{(i,j)})_{i\in[T_1],j\in[T_2]} \parallel \mathsf{id} \parallel \mathsf{m})$. Otherwise abort.
6. Let $\sigma = ((F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]})$.

We show that Game_1 and Game_2 are identical unless the aborting event occurs. All signatures generated by $\mathsf{O}_{\mathsf{Sign}}$ in Game_2 are valid, because $\mathsf{O}_{\mathsf{Sign}}$ computes

- $\hat{F}_1^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_1^{(ch_i)}$ and $\hat{F}_2^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_2^{(ch_i)}$ if $\widehat{ch}_{i,j} = 0$, and
- $\hat{F}_1^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_1^{(i,\widehat{ch}_{i,j})}$ and $\hat{F}_2^{(i,j)} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_2^{(i,\widehat{ch}_{i,j})}$ if $\widehat{ch}_{i,j} > 0$.

That is, the Vrfy algorithm always accepts a signature generated by $\mathsf{O}_{\mathsf{Sign}}$ since Vrfy computes the values above in the same way as $\mathsf{O}_{\mathsf{Sign}}$. Then, the distributions of $\hat{F}_1^{(i,j)}$ and $\hat{F}_2^{(i,j)}$ are uniform, since $\widehat{resp}_{i,j}$ and $\widehat{ch}_i$ are uniformly random (where $i \in [T_1]$ and $j \in [T_2]$). Hence, as long as the aborting event does not occur, Game_2 is identical to Game_1.

In the same way as the proof of the indistinguishability between Game_0 and Game_1, the probability of aborting is at most $(q_s+q_k)(q_s+q_k+q_{\hat{h}}+1)/N$. Therefore, we obtain $|\Pr[W_1]-\Pr[W_2]| \leq (q_s+q_k)(q_s+q_k+q_{\hat{h}}+1)/N$.

$\underline{\mathsf{Game}_3}$: This game is the same as Game_2 except that the challenger generates $E_1^{(i)} = \mathfrak{g}^{a_i} \star E_1^{(0)}$ and $E_2^{(i)} = \mathfrak{g}^{a'_i} \star E_2^{(0)}$ for $i \in [S_0]$ instead of $E_1^{(i)} = \mathfrak{g}^{a_i} \star E_1^{(0)}$ and $E_2^{(i)} = \mathfrak{g}^{a_i} \star E_2^{(0)}$, when generating a master public key and a master secret key.

It is possible to show the indistinguishability between Game_2 and Game_3, by constructing a PPT reduction algorithm solving the $\mathsf{FCMD\text{-}CSIDH}$ problem. In both Game_2 and Game_3, the $\mathsf{O}_{\mathsf{KeyDer}}$ and $\mathsf{O}_{\mathsf{Sign}}$ oracles can be simulated without msk. Thus, it is possible to set the given $\mathsf{FCMD\text{-}CSIDH}$ instance as mpk. Then, if the given values are valid $\mathsf{FCMD\text{-}CSIDH}$ instances, Game_2 can be simulated. If those values are random $\mathsf{FCMD\text{-}CSIDH}$ instances, Game_3 is also simulated. Hence, by using $\mathcal{A}$, we can construct a PPT algorithm $\mathcal{B}$ solving the $\mathsf{FCMD\text{-}CSIDH}$ problem such that $|\Pr[W_2]-\Pr[W_3]| \leq \mathsf{Adv}^{\mathsf{FCMD\text{-}CSIDH}}_{\mathcal{B},S_0}(\lambda)$, in the straightforward way.

We show that the winning probability in Game_3 is negligible. In order to do this, we consider the following two events:

- [Reuse]: $\mathcal{A}$ generates a valid forgery $(\mathsf{id}^*, \mathsf{m}^*, \sigma^*)$ (where $\sigma^* = ((F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}^*_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]})$), by reusing some commitment $(F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}$ generated by $\mathsf{O}_{\mathsf{Sign}}$. Namely, $(F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]} = (F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}$.
- [$\neg\mathsf{Reuse}$]: $\mathcal{A}$ generates a valid forgery $(\mathsf{id}^*, \mathsf{m}^*, \sigma^*)$ (where $\sigma^* = ((F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}^*_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]})$), without reusing any $(F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}$ obtained by $\mathsf{O}_{\mathsf{Sign}}$ given $(\mathsf{id}^*, \mathsf{m}^*)$. Namely, $(F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]} \neq (F_1^{(i,j)}, F_2^{(i,j)})_{i\in[T_1],j\in[S_1]}$.

We first estimate the upper bound of the probability $\Pr[W_3 \wedge \neg\mathsf{Reuse}]$. In order to do this, for the generated public key $\mathsf{mpk} = ((E_1^{(0)}, E_2^{(0)}), (E_1^{(i)} = \mathfrak{g}^{a_i} \star E_1^{(0)}, E_2^{(i)} = \mathfrak{g}^{a'_i} \star E_2^{(0)})_{i\in[S_0]})$, we define $\mathcal{X}_{\mathsf{bad}}$ as the subset of $\mathcal{X}$ (the statement set of lossy CSI-FiSh) which satisfies the following condition for all distinct $i,j \in [S_0]$: $a_i \neq a'_i \wedge a_j - a_i \neq a'_j - a'_i$. Then, for each $(a_i, a'_i) \in (\mathbb{Z}_N)^2$ $(i \in [S_0])$, there are at most $N(N-i)$ pairs satisfying this condition. Hence, $|\mathcal{X}_{\mathsf{bad}}| = N^{S_0+2}(N-1)\cdots(N-S_0)$ holds, and we have $\Pr[\mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] = (N-1)\cdots(N-S_0)/N^{S_0}$.

We estimate the upper bound of the winning probability in the case where the event $[\neg\mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}]$ occurs. Let $\sigma^* = ((F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}^*_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]})$ be the signature generated by $\mathcal{A}$. Note that $H((F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]} \parallel \mathsf{id}^*) = (ch_i^*)_{i\in[T_1S_1]}$ and $\hat{H}((\hat{F}_1^{(i,j)*}, \hat{F}_2^{(i,j)*})_{i\in[T_1],j\in[T_2]} \parallel$

$\mathsf{id}^* \parallel \mathsf{m}^*) = (\widehat{ch}^*_{i,j})_{i\in[T_1],j\in[T_2]}$ are defined, due to the definition of Game_3. We consider the case $\widehat{ch}_{i,j} = 0$ and assume that there exist two hash values $(ch^*_i)_{i\in[T_1S_1]}$ and $(ch_i)_{i\in[T_1S_1]}$ such that the corresponding values $(\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]}$ and $(\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]}$ satisfy the condition of Vrfy. Then, we have

$$\begin{aligned}
&\begin{cases} \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star E_1^{(ch^*_i)}, \ \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star E_2^{(ch^*_i)}, \\ \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_1^{(ch_i)}, \ \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star E_2^{(ch_i)}, \end{cases} \\
\Leftrightarrow\ & E_1^{(ch^*_i)} = \mathfrak{g}^{\widehat{resp}_{i,j} - \widehat{resp}^*_{i,j}} \star E_1^{(ch_i)}, \quad E_2^{(ch^*_i)} = \mathfrak{g}^{\widehat{resp}_{i,j} - \widehat{resp}^*_{i,j}} \star E_2^{(ch_i)}.
\end{aligned}$$

This contradicts the condition of $\mathcal{X}_{\mathsf{bad}}$. We consider the case $\widehat{ch}^*_{i,j} > 0$ and assume that there exist the two hash values $(ch^*_i)_{i\in[T_1S_1]}$ and $(ch_i)_{i\in[T_1S_1]}$ such that the corresponding values $((resp^*_{i,j})_{i\in[T_1].j\in[S_1]}, (\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]})$ and $((resp_{i,j})_{i\in[T_1].j\in[S_1]}, (\widehat{resp}_{i,j})_{i\in[T_1],j\in[T_2]})$ satisfy the acceptance condition of Vrfy. Due to the change of Game_1, we have

$$\begin{aligned}
&\begin{cases} \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star F_1^{(i,\widehat{ch}^*_{i,j})*}, \quad \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star F_2^{(i,\widehat{ch}^*_{i,j})*}, \\ \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_1^{(i,\widehat{ch}_{i,j})}, \quad \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j}} \star F_2^{(i,\widehat{ch}_{i,j})}. \end{cases} \\
\Leftrightarrow\ &\begin{cases} \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j} + resp^*_{i,j}} \star E_1^{(ch^*_i)}, \quad \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j} + resp^*_{i,j}} \star E_2^{(ch^*_i)}, \\ \hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j} + resp_{i,j}} \star E_1^{(ch_i)}, \quad \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}_{i,j} + resp_{i,j}} \star E_2^{(ch_i)}. \end{cases} \\
\Leftrightarrow\ & E_1^{(ch^*_i)} = \mathfrak{g}^{(\widehat{resp}_{i,j} + resp_{i,j}) - (\widehat{resp}^*_{i,j} + resp^*_{i,j})} \star E_1^{(ch_i)}, \quad E_2^{(ch^*_i)} = \mathfrak{g}^{(\widehat{resp}_{i,j} + resp_{i,j}) - (\widehat{resp}^*_{i,j} + resp^*_{i,j})} \star E_2^{(ch_i)}.
\end{aligned}$$

This also contradicts the condition of $\mathcal{X}_{\mathsf{bad}}$. Hence, there exists at most one $(ch^*_i)_{i\in[T_1S_1]}$ that satisfies the condition of Vrfy, and we have $\Pr[W_3 \mid \neg\mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] \le 1/(S_0+1)^{T_1S_1}$. Therefore, we obtain

$$\begin{aligned}
\Pr[W_3 \wedge \neg\mathsf{Reuse}] &= \Pr[W_3 \wedge \neg\mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] + \Pr[W_3 \wedge \neg\mathsf{Reuse} \wedge \mathsf{mpk} \notin \mathcal{X}_{\mathsf{bad}}] \\
&\le \Pr[W_3 \mid \neg\mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] \cdot \Pr[\mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] + \Pr[\mathsf{mpk} \notin \mathcal{X}_{\mathsf{bad}}] \\
&\le \frac{1}{(S_0+1)^{T_1S_1}} \cdot \frac{(N-1)\cdots(N-S_0)}{N^{S_0}} + \left(1 - \frac{(N-1)\cdots(N-S_0)}{N^{S_0}}\right).
\end{aligned}$$

Next, we estimate the upper bound of the probability $\Pr[W_3 \wedge \mathsf{Reuse}]$. Let $\sigma^* = ((F_1^{(i,j)*}, F_2^{(i,j)*})_{i\in[T_1],j\in[S_1]}, (\widehat{ch}^*_{i,j})_{i\in[T_1],j\in[T_2]}, (\widehat{resp}^*_{i,j})_{i\in[T_1],j\in[T_2]})$ be the signature on $(\mathsf{id}^*, \mathsf{m}^*)$, which is generated by $\mathcal{A}$. If $\widehat{ch}^*_{i,j} = 0$, we have

$$\hat{F}_1^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star E_1^{(ch^*_i)}, \ \hat{F}_2^{(i,j)*} = \mathfrak{g}^{\widehat{resp}^*_{i,j}} \star E_2^{(ch^*_i)}.$$

Thus, $\mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}$ always holds since $a_{ch^*_i} \neq a'_{ch^*_i}$ in Game_3.

If $\widehat{ch}^*_{i,j} > 0$, it is shown that there exists at most one $(ch^*_i)_{i\in[T_1S_1]}$ which satisfies the winning condition, in the same way as the case $[W_3 \wedge \neg\mathsf{Reuse}]$.

Hence, it holds that

$$\begin{aligned}
\Pr[W_3 \wedge \mathsf{Reuse}] &= \Pr[W_3 \wedge \mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] + \Pr[W_3 \wedge \mathsf{Reuse} \wedge \mathsf{mpk} \notin \mathcal{X}_{\mathsf{bad}}] \\
&\le \Pr[W_3 \mid \mathsf{Reuse} \wedge \mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] \cdot \Pr[\mathsf{mpk} \in \mathcal{X}_{\mathsf{bad}}] \\
&\le \frac{1}{(S_0+1)^{T_1S_1}} \cdot \frac{(N-1)\cdots(N-S_0)}{N^{S_0}}.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
\Pr[W_3] &= \Pr[W_3 \wedge \mathsf{Reuse}] + \Pr[W_3 \wedge \neg\mathsf{Reuse}] \\
&\le \frac{2}{(S_0+1)^{T_1S_1}} \cdot \frac{(N-1)\cdots(N-S_0)}{N^{S_0}} + \left(1 - \frac{(N-1)\cdots(N-S_0)}{N^{S_0}}\right).
\end{aligned}$$

From the discussion above, the inequality

$$\begin{aligned}\mathsf{Adv}^{\text{euf-id-cma}}_{\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}},\mathcal{A}}(\lambda) &\leq \sum_{i=0}^{2} |\Pr[W_i] - \Pr[W_{i+1}]| + \Pr[W_3] \\ &\leq \mathsf{Adv}^{\mathsf{FCMD\text{-}CSIDH}}_{\mathcal{B},S_0}(\lambda) + \frac{(q_s+q_k)(2q_s+2q_k+q_h+q_{\hat{h}}+2)}{N} \\ &\quad + \frac{2}{(S_0+1)^{T_1 S_1}} \cdot \frac{(N-1)\cdots(N-S_0)}{N^{S_0}} + \left(1 - \frac{(N-1)\cdots(N-S_0)}{N^{S_0}}\right)\end{aligned}$$

is obtained. □

Finally, we have the following result due to Lemma 1 and Theorem 1:

Corollary 1. *If the* D-CSIDH *assumption holds, then the IBS scheme* $\mathsf{IBS}_{\mathsf{LCSI\text{-}FiSh}}$ *is* EUF-ID-CMA *secure in the random oracle model.*

Acknowledgements. This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan. This work was in part supported by JSPS KAKENHI Grant Number JP22H03590.

References

1. Abdalla, M., Fouque, P., Lyubashevsky, V., Tibouchi, M.: Tightly secure signatures from lossy identification schemes. J. Cryptol. **29**(3), 597–631 (2016)
2. Atapoor, S., Baghery, K., Cozzo, D., Pedersen, R.: CSI-SharK: CSI-FiSh with sharing-friendly keys. Cryptology ePrint Archive (2022)
3. Bellare, M., Neven, G.: Multi-signatures in the plain public-key model and a general forking lemma. In: CCS. pp. 390–399. ACM (2006)
4. Beullens, W., Disson, L., Pedersen, R., Vercauteren, F.: CSI-RAShi: Distributed key generation for CSIDH. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings. pp. 257–276. Springer (2021)
5. Beullens, W., Katsumata, S., Pintore, F.: Calamari and falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In: Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II. pp. 464–492. Springer (2020)
6. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: efficient isogeny based signatures through class group computations. In: Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part I. pp. 227–247. Springer (2019)
7. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive (2022)
8. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: 24th Annual International Conference on Theory and Application of Cryptology and Information Security, ASIACRYPT 2018. pp. 395–427. Springer (2018)
9. Childs, A., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology **8**(1), 1–29 (2014)
10. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive (2006)
11. Cozzo, D., Smart, N.P.: Sashimi: cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol. In: Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11. pp. 169–186. Springer (2020)
12. De Feo, L., Galbraith, S.D.: SeaSign: compact isogeny signatures from class group actions. In: Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38. pp. 759–789. Springer (2019)

13. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: ASIACRYPT (1). LNCS, vol. 12491, pp. 64–93. Springer (2020)
14. El Kaafarani, A., Katsumata, S., Pintore, F.: Lossy CSI-FiSh: Efficient signature scheme with tight reduction to decisional CSIDH-512. In: Public Key Cryptography (2). LNCS, vol. 12111, pp. 157–186. Springer (2020)
15. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: countering SIDH attacks by masking information. Cryptology ePrint Archive (2023)
16. Fukumitsu, M., Hasegawa, S.: A galindo-garcia-like identity-based signature with tight security reduction, revisited. In: CANDAR. pp. 92–98. IEEE Computer Society (2018)
17. Galindo, D., Garcia, F.D.: A schnorr-like lightweight identity-based signature scheme. In: AFRICACRYPT. LNCS, vol. 5580, pp. 135–148. Springer (2009)
18. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4. pp. 19–34. Springer (2011)
19. Leroux, A.: A new isogeny representation and applications to cryptography. In: Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part II. pp. 3–35. Springer (2023)
20. Maino, L., Martindale, C.: An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive (2022)
21. NIST: National Institute of Standards and Technology Interagency. `https://doi.org/10.6028/NIST.IR.8413` (2022), [Online; July 2022]
22. Peng, C., Chen, J., Zhou, L., Choo, K.R., He, D.: CsiIBS: A post-quantum identity-based signature scheme based on isogenies. Journal of information Security and Applications **54**, 102504 (2020)
23. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. **13**(3), 361–396 (2000)
24. Robert, D.: Breaking SIDH in polynomial time. Cryptology ePrint Archive (2022)
25. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive (2006)
26. Shamir, A.: Identity-based cryptosystems and signature schemes. In: CRYPTO. LNCS, vol. 196, pp. 47–53. Springer (1984)
27. Shaw, S., Dutta, R.: Identification scheme and forward-secure signature in identity-based setting from isogenies. In: ProvSec. LNCS, vol. 13059, pp. 309–326. Springer (2021)
28. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)
29. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer (2009)
30. Zhang, X., Liu, S., Gu, D., Liu, J.K.: A generic construction of tightly secure signatures in the multi-user setting. Theor. Comput. Sci. **775**, 32–52 (2019)