SQIAsignHD: SQIsignHD Adaptor Signature

Farzin Renan[1] and Péter Kutas[2]

[1] *Middle East Technical University, Ankara, Turkey*
farzin.renan@gmail.com

[2] *University of Birmingham, UK*
[2] *Eötvös Loránd University, Budapest, Hungary*
p.kutas@bham.ac.uk

Abstract

Adaptor signatures can be viewed as a generalized form of the standard digital signature schemes where a secret randomness is hidden within a signature. Adaptor signatures are a recent cryptographic primitive and are becoming an important tool for blockchain applications such as cryptocurrencies to reduce on-chain costs, improve fungibility, and contribute to off-chain forms of payment in payment-channel networks, payment-channel hubs, and atomic swaps. However, currently used adaptor signature constructions are vulnerable to quantum adversaries due to Shor's algorithm. In this work, we introduce SQIAsignHD, a new quantum-resistant adaptor signature scheme based on isogenies of supersingular elliptic curves, using SQIsignHD - as the underlying signature scheme - and exploiting the idea of the artificial orientation on the supersingular isogeny Diffie-Hellman key exchange protocol, SIDH, as the underlying hard relation. We, furthermore, show that our scheme is secure in the Quantum Random Oracle Model (QROM).

Keywords: Post-quantum Cryptography, Blockchain, Isogeny-based Cryptography, Adaptor Signature, Payment Channel Network

Acknowledgements

We would like to show our gratitude to Luca De Feo, Andrea Basso, Simon-Philipp Merz, and the cryptography research group at IBM, for their insightful feedback, and thank the anonymous reviewers for their remarks which helped to improve this paper.

1 Introduction

Blockchain technology, which has been sparking widespread attention since it was introduced anonymously in 2009 due to [1], proposes a novel payment paradigm in which financial transactions are maintained in a decentralized data structure. Each transaction on the blockchain can be treated as a scripting language that is validated by nodes through a decentralized consensus protocol. Cryptocurrencies such as Bitcoin and Ethereum are powered by blockchain technologies. Transactions on blockchains, however, can be quite costly since a user who wants to deploy and execute a transaction must pay a fee to the miners. The fee is calculated based on the storage and computational costs associated with running each transaction script. To address this issue, one way to reduce transaction size is to manage some transactions off-chain to lower the on-chain fee paid to nodes. In this context, Andrew Polestra proposed first the concept of scriptless scripts [2], which was later formalized as adaptor signatures due to [3] and [4].

1.1 Adaptor Signature

Adaptor signature is a recent cryptographic primitive that can be viewed as a generalization of a standard digital signature and becoming an important tool for blockchain applications such as cryptocurrencies to reduce on-chain costs, improve fungibility, and contribute to off-chain forms of payment in payment-channel networks (PCNs), payment-channel hubs (PCHs), and atomic swaps [5]. In terms of technical aspects, in an adaptor signature, secret randomness is concealed by embedding it in the signature during the signing process, which is exposed once the signature is created. More precisely, the typical procedure is to build a pre-signature in the first phase, then turn it into a full signature using secret randomness, and finally extract secret randomness from the signature using cryptographic processing. Furthermore, the signature produced by an adaptor signature can be verified by using the underlying signature scheme's verification algorithm.

An adaptor signature also has specific features that ensure its security. A signer with a secret key can create a pre-signature on every message. This pre-signature can be converted into a full signature on a message if and only if the user has a witness to the statement. In addition, anyone who has access to the pre-signature and the corresponding full signature can extract the witness and reveal the hard relation.

1.2 Related Work and Our Contribution

As concrete instances, Aumayr et al. [3] give a formalization of adaptor signatures and their security, and apply it to ECDSA and Schnorr-based schemes. Malavolta et al. [5] analyze and design secure and privacy-preserving PCNs, identifying a new attack that affects major PCNs like the Lightning Network. They define Anonymous Multi-hop Locks (AMHLs), a cryptographic primitive, and show they can be constructed for PCNs with script languages using linear homomorphic one-way functions. Moreno-Sanchez et al. [6] demonstrate an instance of adaptor signature on the Monero's linkable ring signature scheme to improve scalability and some other issues. Tairi et al. [7] introduce the PCHs protocol and a provably secure instantiation based on adaptor signatures. However, these constructions are vulnerable to quantum adversaries due to Shor's algorithm [8]. More exactly, the security of blockchain technologies primarily is based on digital signature schemes, built on elliptic curve cryptography (ECC), to authenticate payment transactions. The security of ECC, in turn, depends on the intractability of computing the discrete logarithm problem which is secure against classical computers. Yet, the advent of Shor's algorithm enabled quantum computers to efficiently compute discrete logarithms in polynomial running time. This situation makes the blockchain susceptible to quantum attacks. Such attacks involve forging signatures and modifying blocks (faking previous transactions). In the case of Bitcoin, for example, this means a person may spend more than they have or steal assets from other users. As a consequence of the drawbacks of public key cryptosystems, post-quantum cryptography began to attract more attention and became an active research area. Since public key cryptography depends on underlying hard mathematical problems, in order to make a cryptosystem secure against quantum adversaries, the underlying problem must be intractable in the quantum setting.

In the context of post-quantum cryptography, the first established post-quantum adaptor signature is LAS [9], which is built on standard lattice assumptions such as Module-LWE and Module-SIS and has a simplified form of Dilithium [10] as its underlying signature. Applications that employ LAS in their structures require zero-knowledge proof to ensure that the extracted witness is of the desired norm and satisfies the hard relation. However, the most efficient variant of such a proof is 53KB [11] in size, resulting in significant off-chain communication costs. From a privacy standpoint, when LAS is utilized inside particular applications, such as establishing PCNs, it can leak non-trivial information, compromising the overall privacy of the architecture. It should also be noted that there was another attempt to design an adaptor signature, named SQI-AS, introduced in [12], using SQISign [13] as the underlying signature. The authors exploit the idea of SIDH [14] to apply the corresponding hard relation in their design. However, due to the devastating attacks [15, 16, 17] on SIDH, the SQI-AS lost its security. It is because of the fact that SQI-AS's adapting algorithm benefits from SIDH-like operation, thereby in the pre-signature phase of the protocol, it is required to publish the image of the torsion points as auxiliary information to realize the adaptation phase while this SIDH-based additional information is one of the main ingredients in breaking the SIDH security, and consequently exposing the secret key isogeny.

The only secure isogeny-based adaptor signature scheme in the literature is IAS [18] using CSI-FiSh [19] as the underlying signature scheme which relies on the security of the key exchange protocol CSIDH [20]. IAS's efficiency has some restrictions as its parameter sizes are based on CSI-FiSh. Specifically, CSI-FiSh operates on a maximum of CSIDH-512 parameters since knowledge of the class group structure is required to efficiently compute the class group action on uniformly random group elements. It is also noted that the CSIDH-512 is relatively slow and vulnerable to a quantum subexponential attack, and the concrete size of parameters required to provide a tangible security level has been a source of concern. Specifically, Bonnetian et al. [21] introduced a quantum algorithm for evaluating CSIDH-512 that uses fewer than 40,000 logical qubits. Peikert [22] utilized Kuperberg's collimation sieve to attack CSIDH, combining classical memory and quantum random access techniques. These attempts demonstrate that the parameters given by the authors of CSIDH do not achieve the requisite quantum security and are subject to controversial debate. It is needed to mention that there exists a new isogeny-based group action of the class group of an imaginary quadratic order on a set of oriented supersingular curves, named SCALLOP proposed by De Feo et al. [23] that aims to solve the scaling problem with CSI-FiSh. Compared to CSIDH, the key advantage of SCALLOP is that it is simple to compute the class-group structure required to uniquely represent and efficiently act on random group elements, as needed in the CSI-FiSh signature scheme. However, SCALLOP requires more computations to execute the group action, making it slower than CSI-FiSh.

Contribution. Considering the above-mentioned situations, this work, as a contribution, aims to construct and introduce a new post-quantum adaptor signature using SQIsignHD [24] as the underlying signature scheme which is the most compact post-quantum digital signature and compared to the other isogeny-based signature schemes, it is generally faster and flexible in its parameter sets. In contrast to IAS, which is confined to a maximum of the CSIDH-512 parameters which in turn are susceptible to quantum subexponential attacks, our scheme scales well to high-security levels. The signature in our construction is approximately 1.5KB in size for $\lambda = 128$ security level. Finally, it is noted that the main technical difficulties in constructing isogeny-based adaptor signatures emerge from the fact that not all post-quantum digital signatures, in particular SQIsignHD, satisfy certain homomorphic properties. Due to [25], it was shown that signature schemes derived from identification (ID) schemes that also satisfy certain homomorphic features can be generically transformed into adaptor signature schemes. To tackle this issue, we apply the concept of "shifting signature by secret randomness" carefully by using several techniques in order to have SQIsignHD adopt this feature. We also deploy the SIDH attacks (the recent algorithmic breakthrough) as the generic algorithm to recover the secret witness during the extraction phase in our construction.

1.3 Organization of the Paper

In Section 2, we give the necessary preliminaries required for Sections 3, and 4 which are the main sections. These preliminaries consist of two main parts. The former half is on the mathematical prerequisites needed for our construction, and the latter is on the cryptographic background as needed ingredients in the next two sections. In Section 3, as the main part of the paper, we introduce a new adaptor signature SQIAsignHD and examine it in detail. In Section 4, we analyze the security aspect of the SQIAsignHD and give formal proof to show its security in the quantum random oracle model.

2 Preliminaries

Notation. A *negligible* function $\mathsf{negl} : \mathbb{N} \to \mathbb{R}$ is a function that, for every $k \in \mathbb{N}$, admits $\mathcal{O}(n^{-k})$ as its upper bound, i.e., there exists $n_0 \in N$, such that for every $n \geq n_0$ it holds that $\mathsf{negl(n)} \leq 1/n^k$. We denote the uniform sampling of the variable x from the set X by $x \xleftarrow{\$} X$. Moreover, we denote a probabilistic polynomial time (PPT) algorithm A on input y, outputs x by $x \leftarrow A(y)$. In case the algorithm A is a deterministic polynomial time (DPT), it is denoted by $x := A(y)$.

2.1 Elliptic Curves and Isogenies

Elliptic Curves. Let $k := \mathbb{F}_q$ be a finite field such that $q = p^n$, for some prime p and positive integer n, with $\mathrm{char}(k) = p \neq 2, 3$. An *elliptic curve* E is a smooth projective variety of genus 1, defined over k, with distinguished rational point $\infty := [0 : 1 : 0]$.

Since E is an elliptic curve, then its discriminant $\Delta(E)$ is nonzero, and its j-invariant $j(E)$ is defined uniquely up to $\overline{\mathbb{F}}_q$-isomorphism. Let l be a positive integer, the *l-tosion subgroup* of an elliptic curve E is defined as $E[l] := \{P \in E(\bar{k}) \mid [l]P = \infty\}$. We say that an elliptic curve E is *supersingular* if there is no nontrivial p-torsion point over $\overline{\mathbb{F}}_p$, i.e., $E[p] = \{\infty\}$. In case of supersingularity of E, $\mathrm{char}(k) = p$ divides $|E(\mathbb{F}_q)| - q - 1$.

Isogenies. An *isogeny* $\varphi : E_1 \to E_2$ is a surjective morphism that maps the point at infinity of E_1 to the point at infinity of E_2. Two elliptic curves E_1, E_2 are *isogenous* over $\mathbb{F}_q$ in case there exists an isogeny between them over $\mathbb{F}_q$. Furthermore, Tate's theorem [26] says that E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$. The *degree* of isogeny φ is the degree of the field extension $[k(E_1) : \varphi^*(k(E_2))]$ where $k(E_i)$ is the function field of E_i, $i = 1, 2$, and φ^* is the pullback of φ defined as $\varphi^* : k(E_2) \to k(E_1)$ where for $f \in k(E_2), \varphi^*(f) := f \circ \varphi$. The isogeny φ is called *separable* in case the field extension is separable. If $\gcd(\deg(\varphi), char(k)) = 1$, then the isogeny is necessarily separable. Since $\varphi(\infty_{E_1}) = \infty_{E_2}$, then $\varphi : E_1(k) \to E_2(k)$ is a group homomorphism. $|\ker(\varphi)| = \deg(\varphi)$ in case φ is separable. Therefore, in our context, an isogeny can be characterized by its kernel. In other words, there is a one-to-one correspondence between separable isogenies (up to an isomorphism of the target curve) and finite (normal) subgroups of $E_1(k)$. We can construct an isogeny from its kernel by using Vélu's formulas [27]. The constructed isogeny is in the form $E \to E/G$ where G is a finite subgroup of E, and the kernel of the constructed isogeny. Since the degree of isogeny is multiplicative, i.e., for isogenies α and β, $\deg(\alpha \circ \beta) = \deg(\alpha)\deg(\beta)$, then for any isogeny ϕ of degree $l = \prod_{i=1}^{n} l_i$, ϕ can be factored as the composition of l_i-isogenies, $1 \le i \le n$ where integers l_i are not necessarily coprime. In case the l_i are pairwise coprime, then reordering of the l_i will produce a different set of isogenies because of the non-commutativity structure of isogenies of supersingular elliptic curves under composition. For $n = 2$, with some considerations, SQISign benefits from this property in commutative type and introduces specific notations for the isogenies involved in the two possible decompositions, and calls them commutative isogeny diagram as shown in Figure 1. More precisely, suppose that l_1, l_2 are two coprime integers and φ is a $l_1 l_2$-isogeny. Then, φ can be decomposed in two ways, namely $\varphi = \psi_2 \circ \varphi_1 = \psi_1 \circ \varphi_2$. In this case, ψ_1 (respectively, ψ_2) is called the *push-forward* of φ_1 (respectively φ_2) through φ_2 (respectively, φ_1), denoted by $\psi_1 = [\varphi_2]_* \varphi_1$ (respectively, $\psi_2 = [\varphi_1]_* \varphi_2$). It can be shown that $\ker(\psi_1) = \varphi_2(\ker(\varphi_1))$, and $\ker(\psi_2) = \varphi_1(\ker(\varphi_2))$. Furthermore, φ_1 (respectively, φ_2) is called the *pull-back* of ψ_1 (respectively ψ_2) through φ_2 (respectively, φ_1), denoted by $\varphi_1 = [\varphi_2]^* \psi_1$ (respectively, $\varphi_2 = [\varphi_1]^* \psi_2$).

$$\begin{tikzcd}
& E_1 \arrow[dr, "\psi_2"] & \\
E_0 \arrow[ur, "\varphi_1"] \arrow[rr, "\varphi"] \arrow[dr, "\varphi_2"'] & & E_3 \\
& E_2 \arrow[ur, "\psi_1"'] &
\end{tikzcd}$$

Figure 1: Commutative Isogeny Diagram.

For a given isogeny $\alpha : E_1 \to E_2$ of degree d, its (unique) *dual* is an isogeny $\hat{\alpha} : E_2 \to E_1$ of degree d such that $\alpha \circ \hat{\alpha} = [d] : E_2 \to E_2$, and $\hat{\alpha} \circ \alpha = [d] : E_1 \to E_1$. An isogeny from an elliptic curve E to itself is called an *endomorphism*. For each $m \in \mathbb{Z}$, the *multiplication-by-m* map, i.e., $[m] : P \mapsto m \cdot P$, and the *Frobenius* map $\pi : (x, y) \mapsto (x^q, y^q)$ of an elliptic curve defined over $E/\mathbb{F}_q$ are examples of endomorphisms. The set of all endomorphisms on E, denoted by $\mathrm{End}(E)$, forms a ring under addition and composition which is called the *endomorphism ring* of E. Every supersingular elliptic curve in characteristic p is isomorphic to a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. It means that each supersingular elliptic curve has an isomorphic representative defined over $\mathbb{F}_{p^2}$. The supersingular ℓ-isogeny graph is the graph whose vertices are the supersingular j-invariants in $\mathbb{F}_{p^2}$, and whose edges are the ℓ-isogenies between them. These graphs are connected [28], essentially undirected (since each ℓ-isogeny has a dual), $(\ell+1)$-regular (there are exactly $\ell + 1$ outgoing edges from each j-invariant), and Ramanujan [29].

2.2 Endomorphism Rings and Quaternion Orders

Quaternion Algebras. Let $a, b \in \mathbb{Q}^*$. A *quaternion algebra* $\mathcal{B}$ over $\mathbb{Q}$ is a four dimensional central simple $\mathbb{Q}$-algebra denoted by $\mathcal{B} := (\frac{a,b}{\mathbb{Q}}) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with basis $1, i, j, k$ such that $i^2 = a$, $j^2 = b$ and $k = ij = -ji$. Let l be a prime. The quaternion algebra $\mathcal{B}_l := \mathcal{B} \otimes_{\mathbb{Q}} \mathbb{Q}_l$ is obtained by extending the scalars of $\mathcal{B}$ from $\mathbb{Q}$ to $\mathbb{Q}_l$, where $\mathbb{Q}_l$ is the set of l-adic numbers (fraction field of l-adic integers $\mathbb{Z}_l$ which is the localization of $\mathbb{Z}$ away from prime l). Also, we can define $\mathcal{B}_\infty := \mathcal{B} \otimes_{\mathbb{Q}} \mathbb{R}$. We say that $\mathcal{B}$ is ramified at l (including $l = \infty$) if $\mathcal{B}_l$ is a division algebra. We are only interested in $\mathcal{B}_{p,\infty}$ which is a quaternion algebra ramified at p and ∞. A *fractional ideal* I is a $\mathbb{Z}$-lattice of rank four which can be written as $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3 + \mathbb{Z}\alpha_4$ for a $\mathbb{Q}$ basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\mathcal{B}$.

Quaternionic Orders. An *order* is a fractional ideal that is also a subring of $\mathcal{B}$. An order $\mathcal{O}$ is *maximal* in case for any other order $\mathcal{O}'$ if $\mathcal{O} \subseteq \mathcal{O}'$, then $\mathcal{O} = \mathcal{O}'$. Let E be an elliptic curve defined over a field of characteristic p with no non-trivial p-torsion points, namely supersingular. Also, let $\mathcal{B}_{p,\infty}$ be a quaternion algebra $\mathcal{B}$ over $\mathbb{Q}$ ramified exactly at p and ∞. The endomorphism algebra of such an elliptic curve is isomorphic to a quaternion algebra ramified at p and ∞, and its endomorphism ring is isomorphic to a maximal order of the corresponding quaternion algebra, i.e., $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathcal{B}_{p,\infty}$, and $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{B}_{p,\infty}$. Conversely, for any maximal order in $\mathcal{B}_{p,\infty}$, there exists a supersingular elliptic curve over a field of characteristic p such that whose endomorphism ring is isomorphic to this maximal order. This, indeed, is a correspondence which is called *Deuring correspondence* studied in [30]. Generally, for a fixed maximal order $\mathcal{O}_0 \cong \mathrm{End}(E_0)$, there exists an equivalence between the category of supersingular elliptic curves under isogenies and the category of left fractional $\mathcal{O}_0$-ideals under homomorphisms of O_0-modules. Constructing a supersingular elliptic curve whose endomorphism ring is isomorphic to a given maximal order of quaternion algebras (one direction of the Deuring correspondence) is known to be polynomial-time over carefully selected base fields. Starting from a maximal order in a quaternion algebra, finding a supersingular elliptic curve with that maximal order as an endomorphism ring is called the *constructive Deuring correspondence*. Let $\mathcal{O} \subseteq \mathcal{B}_{p,\infty} \cong \mathrm{End}^0(E)$ be a maximal

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\psi_1"'] & E^{'} \arrow[d, "\psi_2"] \\ E_1 & E_2 \end{tikzcd}$$

Figure 2: Parallel Isogenies

order. Given I, an integral left $\mathcal{O}$-ideal, we define the set of I-torsion points of E as $E[I] := \{P \in E : \alpha(P) = 0 \text{ for all } \alpha \in I\}$ as the kernel of I. For the ideal I, we associate isogeny φ_I with kernel $E[I]$ and define it as $\varphi_I : E \to E_I := \frac{E}{E[I]}$.

2.3 Artificial Orientation

We now consider the concept of artificial orientation introduced in [31] to provide a new technique of securely computing SIDH-like operations against current SIDH attacks. For smooth, square-free, and relatively prime integers A and B, let p be a prime of the from $p = ABf - 1$, where f is a small cofactor specifying the p to be prime. Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Then, an *artificial A-orientation* of E is a pair $\mathfrak{A} = (G_1, G_2)$, where G_1, G_2 are cyclic subgroups of $E[A]$, $|G_1| = |G_2| = A$, and $G_1 \cap G_2 = \{0\}$. In this case, the pair $(E, \mathfrak{A})$ is said to be an *artificially A-oriented* curve. For an artificially A-oriented curve $(E, \mathfrak{A})$, a range of isogenies can be computed with kernels derived from $\mathfrak{A} = (G_1, G_2)$. Particularly, an isogeny ϕ is called *$\mathfrak{A}$-isogeny* in case its kernel can be written as the direct sum of a subgroup $H_1 \subseteq G_1$, and a subgroup $H_2 \subseteq G_2$, i.e., $\ker(\phi) = H_1 \oplus H_2$. In this case, ϕ can be decomposed into two relatively prime degrees isogenies ϕ_1, ϕ_2, i.e., $\phi = \phi_2 \circ \phi_1$, where $\ker(\phi_1) = H_1 \subseteq G_1$, $\ker(\phi_2) = \phi_1(H_2) \subseteq \phi_1(G_2)$.

However, as described in [31], for an artificially A-oriented curve $(E, \mathfrak{A})$, and a non-trivial $\mathfrak{A}$-isogeny $\phi : E \to E^{'}$, the artificial A-orientation on E may not always be carried onto $E^{'}$ via the isogeny ϕ since at least one of the subgroups $\phi(G_1)$ and $\phi(G_2)$ of $E^{'}[A]$ may have order smaller than A. To remedy this issue, the degree of the isogeny considered must be relatively prime to A. We, formally, have the following definition, as given in [31], as follows:

Definition 2.1. *For two artificially A-oriented curves $(E, \mathfrak{A})$ and $(E^{'}, \mathfrak{A}^{'})$, and an integer B relatively prime to the A, the pairs is said to be B-isogenous in case there exists a B-isogeny $\phi : E \to E^{'}$ such that*

$$\mathfrak{A}^{'} = (G_1^{'}, G_2^{'}) = \phi(G_1, G_2) = \phi(\mathfrak{A}).$$

Assuming fixed generators $\langle P_1 \rangle = G_1$ and $\langle P_2 \rangle = G_2$, the subgroups $G_1^{'}$ and $G_2^{'}$ can be represented by $[\alpha]\phi(P_1)$ and $[\beta]\phi(P_2)$ respectively, for some $\alpha, \beta \in \mathbb{Z}/A\mathbb{Z}$. Therefore, for a supersingular curve, it is possible to define an artificial orientation on it. Artificial orientations, while not generating a commutative group action like standard orientations, as introduced in [32], offer sufficient information for computing parallel isogenies. Concretely, for given two A-oriented curves $(E, \mathfrak{A})$ and $(E^{'}, \mathfrak{A}^{'})$ connected by a $\mathfrak{B}$-isogeny $\phi : E \to E^{'}$, where $\mathfrak{A} = (G_1, G_2)$ and $\mathfrak{A}^{'} = (G_1^{'}, G_2^{'})$, the isogenies $\psi_1 : E \to E_1$, and $\psi_2 : E^{'} \to E_2$, are parallel as shown in Figure 2, where $E_1 := E/\langle [A_1]G_1 + [A_2]G_2 \rangle$, and $E_2 := E^{'}/\langle [A_1]G_1^{'} + [A_2]G_2^{'} \rangle$, i.e., we have $\ker(\psi_2) = \phi(\ker(\psi_1))$ and the codomain curves are also B-isogenous, connected by the isogeny ϕ' with $\ker(\phi') = \psi_1(\ker(\phi))$. Thus, the isogenies ψ_1 and ψ_2 are characterized by the multiplicative decompositions of A as $A = A_1A_2$. We benefit from the properties of the notion of artificial orientation to construct the pre-signature and adaptation phases of our scheme.

2.4 Computational Hardness Assumptions

Our hardness assumptions, which are derived from the generic hard problem of finding an isogeny between two isogenous elliptic curves defined over a field k, are given below and are supposed to be computationally infeasible problems and applied in the pre-signing and adaptation phases of our scheme.

Problem 2.2 (Supersingular Smooth Endomorphism Problem [13])**.** *Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find a (non-trivial) cyclic endomorphism of E of smooth degree.*

Problem 2.3 (SSIP-A [31])**.** *Let $(E, \mathfrak{B})$ be an artificially B-oriented curve and let A be an integer coprime to B. Let $\phi : E \to E^{'}$ be a cyclic isogeny of degree A and let $\mathfrak{B}^{'} = \phi(\mathfrak{B})$. Given $(E, \mathfrak{B})$ and $(E^{'}, \mathfrak{B}^{'})$ and the degree A, compute ϕ.*

Problem 2.4 (SSIP-B [31])**.** *Let $(E, \mathfrak{B})$ be an artificially B-oriented curve and let A be an integer coprime to B. Let $\psi : E \to E^{'}$ be a cyclic $\mathfrak{B}$-isogeny of degree B, with $A < B$. Let also P, Q be a basis of $E[A]$. Given $(E, \mathfrak{B})$, together with the points P, Q, and the curve E' with the points $\psi(P)$ and $\psi(Q)$, compute ψ.*

2.5 Adaptor Signature Scheme

Hard Relation. Let us first recall the definition of a cryptographically hard relation:

Definition 2.5 (Hard Relation)**.** *Let the subset $\mathsf{R} \subseteq \mathsf{W} \times \mathsf{S}$ be a relation set of witness/statement pairs (w, s). We define the language of R to be the set $\mathcal{L}_{\mathsf{R}} := \{\mathsf{s} \mid \exists \mathsf{w} \text{ s.t. } (\mathsf{w}, \mathsf{s}) \in \mathsf{R}\}$ of valid statements. The relation R is said to be a hard relation in case the following are satisfied:*

- *There exists a PPT sampling algorithm $\mathsf{GenR}(1^\lambda)$ taking the security parameter λ as input, and outputs a witness/statement pair $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$.*
- *The validation of the relation is decidable in polynomial running time.*
- *For any PPT adversary $\mathcal{A}$, a negligible function negl exists such that:*

$$Pr\left[(\mathsf{w}^*, \mathsf{s}) \in \mathsf{R} \;\middle|\; \begin{array}{c} (\mathsf{w}, \mathsf{s}) \leftarrow \mathsf{GenR}(1^\lambda) \\ \mathsf{w}^* \leftarrow \mathcal{A}(\mathsf{s}) \end{array} \right] \leq \mathsf{Negl}(\lambda),$$

where the probability comes from the randomness of GenR and $\mathcal{A}$.

Non-interactive Proof System. Let $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$ be cryptographically a hard relation, and $\mathcal{H}$ be a random oracle. A *non-interactive proof system* is a pair (P, V) of two PPT oracle algorithms:

- $\pi_{\mathsf{w}}/\perp \leftarrow \mathsf{P}^{\mathcal{H}}(\mathsf{w},\mathsf{s})$: a prover P taking a pair $(\mathsf{w},\mathsf{s}) \in \mathsf{R}$ as input and outputting a proof π_{w} of the statement s with witness w. $\mathsf{P}^{\mathcal{H}}(\mathsf{w},\mathsf{s}) = \perp$ if $(\mathsf{w},\mathsf{s}) \notin \mathsf{R}$.
- $0/1 \leftarrow \mathsf{V}^{\mathcal{H}}(\mathsf{s},\pi_{\mathsf{w}})$: a verifier V taking a pair $(\mathsf{s},\pi_{\mathsf{w}})$ and outputting whether it accepts or rejects the proof π_{w} of s.

which satisfies the following conditions:

i. Completeness: Let $(\mathsf{w},\mathsf{s}) \in \mathsf{R}$ and $\pi_{\mathsf{w}} \leftarrow \mathsf{P}^{\mathcal{H}}(\mathsf{w},\mathsf{s})$, then there exists a negligible function negl such that $\Pr[\mathsf{V}^{\mathcal{H}} = 1] \geq 1 - \mathsf{negl}(\lambda)$.

ii. Zero-knowledge (NIZK): For a PPT algorithm $\mathcal{S}$, the zero-knowledge simulator, and for any pair (w,s) and PPT algorithm $\mathcal{D}$ the following distributions are computationally indistinguishable:

   - $\pi_{\mathsf{w}} \leftarrow \mathsf{P}^{\mathcal{H}}(\mathsf{w},\mathsf{s})$ if $(\mathsf{w},\mathsf{s}) \in \mathsf{R}$ and $\pi_{\mathsf{w}} \leftarrow \perp$ otherwise. Output $\mathcal{D}^{\mathcal{H}}(\mathsf{w},\mathsf{s},\pi_{\mathsf{w}})$.
   - $\pi_{\mathsf{w}} \leftarrow \mathcal{S}(\mathsf{s},1)$ if $(\mathsf{w},\mathsf{s}) \in \mathsf{R}$ and $\pi_{\mathsf{w}} \leftarrow \mathcal{S}(\mathsf{s},0)$ otherwise. Output $\mathcal{D}^{\mathcal{H}}(\mathsf{w},\mathsf{s},\pi_{\mathsf{w}})$.

iii. Online-extractability: For a PPT algorithm $\mathcal{E}$, the online extractor, and for any algorithm A, let $(\mathsf{s},\pi_{\mathsf{w}}) \leftarrow \mathsf{A}^{\mathcal{H}}(\lambda)$ be the sequence of queries of A to $\mathcal{H}$ and H_A be the $\mathcal{H}$'s answers. Let $\mathsf{w} \leftarrow \mathcal{E}(\mathsf{s},\pi_{\mathsf{w}},\mathsf{H_A})$. Then it holds that

$$\Pr[(\mathsf{w},\mathsf{s}) \notin \mathsf{R} \wedge \mathsf{V}^{\mathcal{H}}(\mathsf{s},\pi_{\mathsf{w}}) = 1] \leq \mathsf{negl}(\lambda).$$

Digital Signature Scheme. We recall the definition of a digital signature scheme and the properties that a signature scheme must satisfy to be called secure.

Definition 2.6 (Digitial Signature Scheme)**.** *A digital signature is a triple scheme* $\Sigma = (\mathsf{KeyGen},\mathsf{Sig},\mathsf{Ver})$ *consisting of three polynomial-time algorithms:*

- $(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$: *a PPT key pairs generating algorithm that takes security parameter λ as its input, and outputs a key pair* $(\mathsf{sk},\mathsf{pk})$*;*

- $\sigma \leftarrow \mathsf{Sig}(\mathsf{sk},m)$: *a PPT signing algorithm that takes a secret key* sk *and message $m \in \{0,1\}^\star$ as input, and outputs a signature σ;*

- $0/1 \leftarrow \mathsf{Ver}(\mathsf{pk},m,\sigma)$: *a DPT verifying algorithm that takes a public key* pk*, message $m \in \{0,1\}^\star$ and signature σ as input, and outputs a bit $b \in \{0,1\}$.*

The first property that each signature scheme must satisfy, to guarantee the correctness of the scheme, is *signature correctness*, i.e., for any security parameter $\lambda \in \mathbb{N}$, and a message $m \in \{0,1\}^*$:

$$\Pr\Big[\mathsf{Ver}(\mathsf{pk},m,\mathsf{Sig}(\mathsf{sk},m)) = 1 \,\Big|\, (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\Big] = 1.$$

There are several definitions of security requirements for a signature scheme. One of the most common of those properties is *existential unforgeability under chosen message attacks*, abbreviated as EUF-CMA. Satisfying this property basically means forging a verifiable signature on a message m without knowing the private key sk is infeasible even in case the PPT adversary has access to many previously produced valid signatures on messages of his choice but message m. The formal definition of this property is as follows:

Definition 2.7 (EUF-CMA Security)**.** *A signature scheme* Σ *is* EUF-CMA *secure if for every* PPT *adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that*

$$Pr[\mathsf{SigForge}_{\mathcal{A},\Sigma}(\lambda) = 1] \leq \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{SigForge}_{\mathcal{A},\Sigma}$ *is defined as follows:*

$\mathsf{SigForge}_{\mathcal{A},\Sigma}(\lambda)$	$\mathcal{O}_S(m)$
$\mathcal{Q} \leftarrow \emptyset$	$\sigma \leftarrow \mathsf{Sig}(\mathsf{sk}, m)$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$	$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
$(m, \sigma) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot)}(\mathsf{pk})$	**return** σ
return $(m \notin \mathcal{Q} \wedge \mathsf{Ver}(\mathsf{pk}, m, \sigma))$	

Furthermore, we have a stronger definition indicating the difficulty of transforming a valid signature on a message m into another valid signature on m, namely *strong existential unforgeability under chosen message attacks*, abbreviated as SUF-CMA. This property guarantees that the adversary is not able even to produce a new signature for a previously signed message, i.e., assume that an adversary obtains a message/signature pair (m, σ) together with some message/signature pairs of his choice, the signature scheme is called SUF-CMA secure in case the adversary cannot produce a new signature σ^* for the message m. Formally, we have the following definition:

Definition 2.8 (SUF-CMA Security)**.** *A signature scheme* Σ *is* SUF-CMA *secure if for every* PPT *adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that*

$$Pr[\mathsf{StrongSigForge}_{\mathcal{A},\Sigma}(\lambda) = 1] \leq \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{StrongSigForge}_{\mathcal{A},\Sigma}$ *is defined as follows:*

$\mathsf{StrongSigForge}_{\mathcal{A},\Sigma}(\lambda)$	$\mathcal{O}_S(m)$
$\mathcal{Q} \leftarrow \emptyset$	$\sigma \leftarrow \mathsf{Sig}(\mathsf{sk}, m)$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$	$\mathcal{Q} := \mathcal{Q} \cup \{m, \sigma\}$
$(m, \sigma) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot)}(\mathsf{pk})$	**return** σ
return $((m, \sigma) \notin \mathcal{Q} \wedge \mathsf{Ver}(\mathsf{pk}, m, \sigma))$	

Adaptor Signature Scheme. An adaptor signature is a cryptographic primitive that can be treated as a generalization of an ordinary digital signature. More precisely, it hides secret randomness within the signature so that the secret randomness is revealed once the signature is generated. The general procedure is that a pre-signature is generated in the first step. Then, the pre-signature is shifted by secret randomness and adapted into a signature. Finally, the secret randomness is extracted from the signature based on cryptographic processing. Furthermore, the signature produced by an adaptor signature is verifiable by the verification algorithm of the underlying signature scheme.

An adapter signature also has some properties to guarantee its security. For any statement $\mathsf{s} \in \mathcal{L}_{\mathsf{R}}$, a signer holding a secret key sk can produce a pre-signature $\tilde{\sigma}$ on any message m. This pre-signature can be adapted into a full signature σ on m if and only if a user has a witness w to the statement s, i.e., $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$. Additionally, anyone with access to the pre-signature $\tilde{\sigma}$, full signature σ, and witness s can extract the witness w and thus reveal the hard relation.

The formal definition of an adaptor signature and its properties are given as follows:

Definition 2.9 (Adaptor Signature Scheme)**.** *An adaptor signature scheme with respect to a hard relation* R *and a signature scheme* $\Sigma = (\mathsf{KeyGen}, \mathsf{Sig}, \mathsf{Ver})$ *is a quadruple* $\Xi_{\mathsf{R},\Sigma} = (\mathsf{PreSig}, \mathsf{PreVer}, \mathsf{Adapt}, \mathsf{Ext})$ *defined as:*

- $\tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s})$: *a* PPT *algorithm that takes a secret key* sk*, message* $m \in \{0,1\}^*$*, and statement* $\mathsf{s} \in \mathcal{L}_{\mathsf{R}}$*, and produces a pre-signature* $\tilde{\sigma}$*.*
- $0/1 \leftarrow \mathsf{PreVer}(\mathsf{pk}, m, \mathsf{s}, \tilde{\sigma})$: *a* DPT *algorithm that takes a public key* pk*, a message* $m \in \{0,1\}^*$*, a statement* $\mathsf{s} \in \mathcal{L}_{\mathsf{R}}$*, and a pre-signature* $\tilde{\sigma}$*, and produces a bit* $b \in \{0,1\}$*.*
- $\sigma \leftarrow \mathsf{Adapt}(\tilde{\sigma}, \mathsf{w})$: *a* DPT *algorithm that takes a valid pre-signature* $\tilde{\sigma}$*, and a witness* w*, and produces a signature* σ*.*
- $\mathsf{w}/\perp \leftarrow \mathsf{Ext}(\sigma, \tilde{\sigma}, \mathsf{s})$: *a* DPT *algorithm that takes a pre-signature* $\tilde{\sigma}$*, a corresponding signature* σ*, and a statement* $\mathsf{s} \in \mathcal{L}_{\mathsf{R}}$*, and produces a witness* w *(to the statement* s*) such that* $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$*, or* $\perp$*.*

For an adaptor signature, KeyGen and Ver algorithms are inherited from the underlying signature scheme Σ; and GenR is based on the underlying hard relation to generate witness/statement pair $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$.

As mentioned before, some properties are required to guarantee the security of an adaptor signature scheme. The first property is *pre-signature correctness* ensuring that an honestly generated pre-signature can be adapted to a signature.

Definition 2.10 (Pre-signature Correctness)**.** *An adaptor signature scheme* $\Xi_{\mathsf{R},\Sigma}$ *satisfies pre-signature correctness if for any* $\lambda \in \mathbb{N}$*, any message* $m \in \{0,1\}^*$*, and any witness/statement pair* (w, s)*, the following holds:*

$$Pr\left[\begin{array}{c|c} \mathsf{PreVer}(\mathsf{pk}, m, \mathsf{s}, \tilde{\sigma}) = 1 & (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \mathsf{Ver}(\mathsf{pk}, m, \sigma) = 1 & \tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s}) \\ (\mathsf{w}', \mathsf{s}) \in \mathsf{R} & \sigma := \mathsf{Adapt}(\tilde{\sigma}, \mathsf{w}) \\ & \mathsf{w}' := \mathsf{Ext}(\sigma, \tilde{\sigma}, \mathsf{s}) \end{array}\right] = 1.$$

The second property required for an adaptor signature is *pre-signature adaptability.* It states that any valid (but not necessarily honestly generated) pre-signature with respect to a statement s can be adapted into a valid signature using the witness w such that $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$.

Definition 2.11 (Pre-signature Adaptability)**.** *An adaptor signature scheme* $\Xi_{\mathsf{R},\Sigma}$ *satisfies pre-signature adaptability if for any* $\lambda \in \mathbb{N}$*, message* $m \in \{0,1\}^*$*, witness/statement* *pair* $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$*, key pair* $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*, and pre-signature* $\tilde{\sigma} \leftarrow \{0,1\}^*$ *such that* $\mathsf{PreVer}(\mathsf{pk}, m, \mathsf{s}, \tilde{\sigma}) = 1$*, the following holds:*

$$Pr[\mathsf{Ver}(\mathsf{pk}, m, \mathsf{Adapt}(\tilde{\sigma}, \mathsf{w})) = 1] = 1.$$

There exists another property that is about the unforgeability of an adaptor signature called *existential unforgeability under chosen message attack*, abbreviated as aEUF-CMA. It states that even in the presence of a pre-signature on a message m with respect to a random statement $\mathsf{s} \in \mathcal{L}_\mathsf{R}$, forging a valid signature σ for m is computationally infeasible for an adversary.

Definition 2.12. *[*$\mathsf{aEUF-CMA}$ *Security] An adaptor signature scheme* $\Xi_{\mathsf{R},\Sigma}$ *is* $\mathsf{aEUF-CMA}$ *secure if for any* PPT *adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that*

$$Pr[\mathsf{aSigForge}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}(\lambda) = 1] \leq \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{aSigForge}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}$ *is defined as follows:*

$$\begin{array}{l}
\underline{\mathsf{aSigForge}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}(\lambda)}\\
\mathcal{Q} := \emptyset\\
(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\
m \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk})\\
(\mathsf{w}, \mathsf{s}) \leftarrow \mathsf{GenR}(1^\lambda)\\
\tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s})\\
\sigma \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\sigma}, \mathsf{s})\\
\textbf{return } m \notin \mathcal{Q} \wedge \mathsf{Ver}(\mathsf{pk}, m, \sigma)
\end{array}
\qquad
\begin{array}{l}
\underline{\mathcal{O}_S(m)}\\
\sigma \leftarrow \mathsf{Sig}(\mathsf{sk}, m)\\
\mathcal{Q} := \mathcal{Q} \cup \{m\}\\
\textbf{return } \sigma\\
\\
\underline{\mathcal{O}_{pS}(m, s)}\\
\tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s})\\
\mathcal{Q} := \mathcal{Q} \cup \{m\}\\
\textbf{return } \tilde{\sigma}
\end{array}$$

The fourth and last property is called *witness extractability* stating that any valid pre-signature/signature pair on a message m with respect to a statement s, suffice to extract the corresponding witness w satisfying $(\mathsf{w}, \mathsf{s}) \in \mathsf{R}$.

Definition 2.13 (Witness Extractability)**.** *An adaptor signature scheme* $\Xi_{\mathsf{R},\Sigma}$ *is witness extractable if for any* PPT *adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that the following holds:*

$$Pr[\mathsf{aWitExt}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}(\lambda) = 1] \leq \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{aWitExt}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}$ *is defined as follows:*

$$\begin{array}{l}
\underline{\mathsf{aWitExt}_{\mathcal{A},\Xi_{\mathsf{R},\Sigma}}(\lambda)}\\
\mathcal{Q} := \emptyset\\
(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\
(m, \mathsf{s}) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk})\\
\tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s})\\
\sigma \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\sigma})\\
\mathsf{w}' := \mathsf{Ext}(\sigma, \tilde{\sigma}, \mathsf{s})\\
\textbf{return } (m \notin \mathcal{Q} \wedge (\mathsf{w}', \mathsf{s}) \notin \mathsf{R} \wedge \mathsf{Ver}(\mathsf{pk}, m, \sigma))
\end{array}
\qquad
\begin{array}{l}
\underline{\mathcal{O}_S(m)}\\
\sigma \leftarrow \mathsf{Sig}(\mathsf{sk}, m)\\
\mathcal{Q} := \mathcal{Q} \cup \{m\}\\
\textbf{return } \sigma\\
\\
\underline{\mathcal{O}_{pS}(m, \mathsf{s})}\\
\tilde{\sigma} \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s})\\
\mathcal{Q} := \mathcal{Q} \cup \{m\}\\
\textbf{return } \tilde{\sigma}
\end{array}$$

As it can be seen, the witness extractability experiment $\mathsf{aWitExt}$ is analogous to the experiment $\mathsf{aSigForge}$. Still, an important difference exists in the sense that the adversary can choose the forgery statement s. Therefore, we can think of this situation as if the adversary knows a witness for s and can generate a valid signature on the forgery message m. But note that this is not sufficient to win the experiment. The adversary wins only in case the valid signature does not reveal a witness for s.

In the light of the above properties on the adaptor signature scheme, we have the following definition:

Definition 2.14 (Secure Adaptor Signature Scheme)**.** *An adaptor signature scheme* $\Xi_{\mathsf{R},\Sigma}$ *is secure, if it is* $\mathsf{aEUF\text{-}CMA}$ *secure, pre-signature adaptable, and witness extractable.*

2.6 SQIsignHD

SQIsignHD [24] is a post-quantum digital signature scheme inspired by SQISign [13] that uses the algorithmic breakthrough from the attacks [15], [16], and [17] on SIDH to efficiently represent isogenies of arbitrary degrees. It scales well to high-security levels, is simpler and more efficient, and has smaller signature sizes than SQISign. The SQIsignHD protocol is as follows:

Let $D_\varphi := \prod_{i=1}^{n} \ell_i^{e_i}$ be a smooth number and $\mu(D_\varphi) := \prod_{i=0}^{n} \ell_i^{e_i-1}(\ell_i+1)$. Also, let $\Phi_{D_\varphi}(E, h)$ be an arbitrary function that maps an integer $h \in [1, \mu(D_c)]$ to a non-backtracking isogeny of degree D_φ starting at E. Consider a hash function $\mathsf{H} : \{0,1\} \to [1, \mu(D_\varphi)]$ which is cryptographically secure.

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\psi"] \arrow[d, dashed, "\tau"'] & E_1 \arrow[d, bend right, "\sigma"'] \\
E_A \arrow[r, "\varphi"'] & E_2
\end{tikzcd}$$

Figure 3: SQIsignHD Protocol

Setup. Choose a prime p and supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ with known endomorphism ring $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ such that E_0 has smooth torsion defined over a small extension of $\mathbb{F}_{p^2}$ of degree 1 or 2.

KeyGen. Generate a random secret isogeny $\tau : E_0 \to E_A$ of fixed smooth degree D_τ. The secret/public key pair is $(\mathsf{sk}, \mathsf{pk}) = (\tau, E_A)$.

Sign. Generate a random (secret) commitment isogeny $\psi : E_0 \to E_1$. Then, for signing a message m, build the isogeny $\Phi_{D_\varphi}(E_A, h) = \varphi : E_A \to E_2$, where $h = \mathsf{H}(j(E_1), m)$. Finally, from the knowledge of the secret key τ, and isogenies φ, ψ, construct an efficient representation $R = (\sigma(P_1), \sigma(P_2), q)$ given by the image of torsion points by a response isogeny $\sigma : E_1 \to E_2$ and return the pair $\Sigma := (E_1, R)$ as a signature.

Verify. Upon receiving a signature $\Sigma = (E_1, R)$ associated with the message m and public key E_A, a verifier first recovers $h = H(j(E_1), m)$ and then $\varphi = \Phi(E_A, h) : E_A \to E_2$, finally checks that R represents correctly an isogeny $\sigma : E_1 \to E_2$ by computing a higher dimensional isogeny, as described in SQIsignHD.

The public parameters for SQIsignHD are easy to generate. Specifically, the underlying prime needs only be of the form $p = c\ell^f \ell'^{f'} - 1$ where $\ell \neq \ell'$ are two primes (which in practice $\ell = 2$ and $\ell' = 3$), $c \in \mathbb{N}^*$ is a small cofactor, and $\ell^f \approx \ell'^{f'} \approx \sqrt{p}$, which is made to ensure sufficient accessible torsion for the isogeny computations. Because of this high flexibility property of the underlying prime p, we are able to replace ℓ^f and $\ell'^{f'}$ with a collection of some small primes, as will be shown in Section 3.1, in order to provide a suitable setting to apply the notion of artificial orientation to our construction.

It should be also noted that the signature, as shown in the protocol, is a data $(E_1, q, \sigma(P_1), \sigma(P_2))$, with $q < \ell^f$, $\sigma : E_1 \to E_2$ a q-isogeny and (P_1, P_2) a basis of $E_1[\ell^f]$. This data is based upon the following definition:

Definition 2.15 ([24]). *Suppose that* A *is an algorithm and* $\varphi : E \to E'$ *is an* $\mathbb{F}_q$*-rational isogeny. Then, an efficient representation of isogeny* φ *(with respect to* A*) is some data* $\mathsf{D} \in \{0,1\}^*$ *such that:*

1. D *has polynomial size in* $\log(\deg(\varphi))$ *and* $\log(q)$.
2. *On input* D *and* $P \in E(\mathbb{F}_{q^k})$, A *returns* $\varphi(P)$ *in polynomial time in* $k\log(q)$ *and* $\log(\deg(\varphi))$.

3 New Adaptor Signature Construction

In this section, we introduce a new post-quantum adaptor signature scheme using SQIsignHD [24] as the underlying signature scheme and exploiting the idea of the artificial orientation, on the supersingular isogeny Diffie-Hellman key exchange protocol (SIDH), introduced as $\mathsf{binSIDH}^{\mathsf{hyb}}$ variant in [31], to apply the corresponding hard relation.

At the moment, the only secure post-quantum isogeny-based adaptor signature is IAS introduced in [18] which is constructed upon CSI-FiSh [19]. IAS has restrictions in terms of efficiency due to its parameter sizes relying on CSI-FiSh. More precisely, CSI-FiSh works on at most the CSIDH-512 parameters since knowledge about the class group structure is required to efficiently compute the class group action on uniformly random group elements. We, now, introduce our post-quantum adaptor signature construction in detail and illustrate our scheme's protocol in Algorithm 1.

3.1 Public Parameters

To deploy our protocol, we need to set some initial parameters. These public parameters are inspired by those used in $\mathsf{binSIDH}^{\mathsf{hyb}}$ and SQIsignHD. Therefore, the setup of our scheme is as follows.

We set a prime p of the from $p = ABCf - 1$ such that $A = 2^a$, $B = \prod_{i=1}^{t} \ell_i$, and $C = 3^c$ are pairwise relatively prime integers, f is some (small) cofactor, ℓ_i's are distinct small primes, where $A \approx p^{3/10}$, $B \approx p^{3/5}$, and $C \approx p^{1/10}$. Let $E_0/\mathbb{F}_{p^2}$ be a supersingular elliptic curve with known endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0 \subset \mathcal{B}_{p,\infty}$, and $|E_0(\mathbb{F}_{p^2})| = (p+1)^2$. Additionally, we assume that $\mathfrak{B} = (G_1, G_2)$ is an artificial B-orientation on E_0, and determine a fixed basis $\langle P, Q\rangle = E_0[C]$. We, furthermore, pick a secure hash function $\mathsf{H} : \{0,1\} \to [1, \mu(D_\varphi)]$ similar to that given in SQIsignHD.

3.2 Key Generation & Hard Relation

The key generation step is identical to the generic procedure in SQIsignHD. More precisely, a random secret isogeny $\tau : E_0 \to E_\tau$ is chosen, thereby the secret/public pair is set as $(\mathsf{sk}, \mathsf{pk}) = (\tau, E_\tau)$.

To define the hard relation in our scheme, we set the witness/statement pairs as follows:

$$\mathsf{R}_{\mathfrak{A}} := \left\{ \Big(w, (E_w, w(\mathfrak{B}))\Big) \;\middle|\; \begin{array}{c} w : E_0 \to E_w := E_0/\langle P + [\alpha]Q\rangle, \\ \text{where } \langle P, Q\rangle = E_0[C], \alpha \in \mathbb{Z}/C\mathbb{Z}. \\ (E_0, \mathfrak{B}) \text{ is artificially } B\text{-oriented.} \end{array} \right\},$$

where w is the secret witness isogeny $w : E_0 \to E_w$ with the artificially B-oriented curve $(E_0, \mathfrak{B})$ as its domain, and the pair $(E_w, w(\mathfrak{B}))$ is the statement consisting of the target elliptic curve E_w, and the image the artificially B-orientation $\mathfrak{B} = (G_1, G_2)$ under witness isogeny w.

3.3 Pre-signature

The procedure of the pre-signing algorithm carries some similarities to that described in the SQIsignHD protocol, however, it differs slightly in producing the commitment isogeny (curve, accordingly), as well as some additional ingredients that are required during the adaption phase.

In some sense (unlike SQIsignHD), in the pre-signature phase, we have two (secret) commitment isogenies: one is used in the pre-signature phase, and the other, which is generated by involving the statement curve, is required for the adaption phase. Let us examine them more closely.

Commitment $\boldsymbol{\psi}$. The first commitment isogeny ψ is a $\mathfrak{B}$-oriented isogeny $\psi : E_0 \to E_\psi$ generated by sampling uniformly at random a vector $\vec{b}$ from $\{1,2\}^t$ to compute $\ker(\psi) := \langle G^1_{b_1}, G^2_{b_2}, \ldots, G^t_{b_t}\rangle$, where $G_1 := \langle G^1_1, G^2_1, \ldots, G^t_1\rangle$ and $G_2 := \langle G^1_2, G^2_2, \ldots, G^t_2\rangle$ and $|G^i_1| = |G^i_2| = \ell_i$, for $1 \le i \le t$. Moreover, by using isogeny ψ, the image of public parameters P and Q is determined. We set these images as $S := (\psi(P), \psi(Q))$.

Commitment $\boldsymbol{\psi'}$. The second commitment isogeny ψ' is obtained via push-forward of the first commitment ψ through the witness $w : E_0 \to E_w$ with the help of the component $w(\mathfrak{B})$ of the public statement that is the image of the artificially B-orientation $\mathfrak{B}$ under the witness isogeny w, i.e, $\psi' := [w]_*\psi : E_w \to E_1$. This way, we obtain the second commitment curve E_1 whose j-invariant is used to compute the challenge isogeny. Lastly, we compute the zero-knowledge proof [1] $\pi_{\psi'}$ showing that E_1 is generated honestly using the parallel isogeny to ψ.

Now, the challenge and pre-signature isogenies are produced as follows:

Challenge $\boldsymbol{\varphi}$. To produce a challenge isogeny, the j-invariant of the second commitment curve E_1, which is obtained from implicitly involving the statement curve E_w, along with a message m induce an isogeny starting at the public key E_τ. Specifically, for $h := \mathsf{H}(j(E_1), m)$, let the challenge isogeny be defined as an isogeny $\varphi := \Phi(E_\tau, h) : E_\tau \to E_2$.
Pre-signature $\tilde{\boldsymbol{\sigma}}$. In order to complete the pre-signing phase of a message m with a secret key isogeny $\tau : E_0 \to E_\tau$, from the knowledge of isogenies τ, φ and ψ, an efficient representation $\mathcal{R}_{\tilde{\sigma}} = (\tilde{\sigma}(R_1), \tilde{\sigma}(R_1), \deg(\tilde{\sigma}))$ is constructed by the image of a canonically determined basis $\langle R_1, R_2 \rangle$ of $E_\psi[A]$ under a pre-signature isogeny $\tilde{\sigma} : E_\psi \to E_2$.

Hence, the pre-signature tuple is defined as $\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$, thereby the pre-signing algorithm is designed as follows:

$$\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}}) \leftarrow \mathsf{PreSig}(\mathsf{sk}, m, \mathsf{s}) = \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big).$$

3.4 Pre-verification

To pre-verify the pre-signature, first, upon receiving the pair $S = (\psi(P), \psi(Q))$ from the pre-signature step, the equality $e_C(\psi(P), \psi(Q)) = e_C(P, Q)^B$ of Weil pairings is checked. Additionally, using the curve E_1, the proof $\pi_{\psi'}$ is verified, i.e., it is checked whether $1 = \mathsf{NIZK.V}(E_1, \pi_{\psi'})$. Finally, after computing $h = \mathsf{H}(j(E_1), m)$ and recovering the challenge isogeny $\varphi = \Phi(E_\tau, h) : E_\tau \to E_2$, it is verified that $\mathcal{R}_{\tilde{\sigma}}$ represents correctly an isogeny $\tilde{\sigma} : E_\psi \to E_2$ by computing a higher dimensional isogeny, as explained in SQIsignHD. In case the above-mentioned conditions are not met, it aborts. Thus, the pre-verification algorithm is defined as follows:

$$0/1 \leftarrow \mathsf{PreVer}(\mathsf{pk}, m, \mathsf{s}, \tilde{\Sigma}) = \mathsf{PreVer}\Big(E_\tau, m, (E_w, w(\mathfrak{B})), (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})\Big).$$

3.5 Adaptation

To adapt the pre-signature into a (full) signature, first the parallel isogeny w' to the witness isogeny w is computed by using the additional information $S = (\psi(P), \psi(Q))$ which is necessarily led to coincide the second commitment curve E_1, i.e., $w' := [\psi]_* w : E_\psi \to E_1$. Next, by deploying an algorithm, denoted by A, in the sense of the Definition 2.15, an efficient representation data is constructed via the image of torsion points under the (full) signature isogeny $\sigma := \tilde{\sigma} \circ \hat{w}' : E_1 \to E_2$ as follows:

[1] Since the response isogeny in SQIsignHD is of a large prime degree $q \approx p^{1/2}$, it is hard to attempt traversing on the supersingular isogeny graph in order to simulate a response isogeny. Yet having a zero-knowledge proof showing that the commitment curve E_1 is honestly generated will be a safer option.

$$\begin{tikzcd}
 & E_w \arrow[rr, "\psi'"] & & E_1 \arrow[ddl, bend left, "\sigma"] \\
E_0 \arrow[ur, "w"] \arrow[rr, "\psi"] \arrow[d, "\tau"'] & & E_\psi \arrow[ur, "w'"] \arrow[d, "\tilde{\sigma}"'] & \\
E_\tau \arrow[rr, "\varphi"'] & & E_2 &
\end{tikzcd}$$

Figure 4: SQIAsignHD Protocol

1. Determine a canonical basis $\langle P_0, Q_0 \rangle = E_1[AC]$.
2. Compute $\hat{w}'(P_0)$ and $\hat{w}'(Q_0)$ by explicit description of isogeny $\hat{w}'$.
3. Compute $\mathsf{A}(\mathcal{R}_{\tilde{\sigma}}, \hat{w}'(P_0)) =: \sigma(P_0)$ and $\mathsf{A}(\mathcal{R}_{\tilde{\sigma}}, \hat{w}'(Q_0)) =: \sigma(Q_0)$.
4. Generate an efficient representation
$$\mathcal{R}_\sigma := \big(\sigma(P_0), \sigma(Q_0), \deg(\sigma)\big)$$
of the isogeny $\sigma : E_1 \to E_2$.

The signature is defined as $\Sigma := (E_1, \mathcal{R}_\sigma)$. Thus, the adapting algorithm is designed as follows:
$$\Sigma := (E_1, \mathcal{R}_\sigma) \leftarrow \mathsf{Adapt}(\tilde{\Sigma}, \mathsf{w}) = \mathsf{Adapt}((E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}}), w).$$

3.6 Extraction

Now, in the last phase of our scheme, in order to extract the secret witness isogeny w by using publicly known pre-signature $\tilde{\Sigma}$ and signature Σ, we exploit two computing approach: one is computing the discrete logarithm (of modulus a sufficiently smooth integer), denoted by $\mathcal{A}_{\mathsf{DLP}}$, and the other is the attack for key recovery of an isogeny satisfying $n^2 > 4d$ via SIDH attack [15], denoted by $\mathcal{A}_{\mathsf{SIDH}}$, where d is the degree of the isogeny and n is the order of the given torsion points information. We, furthermore, make use of the algorithm A in the sense of the Definition 2.15. Therefore, the extraction process follows the following steps:

1. Determine a canonical basis $\langle P_1, Q_1 \rangle = E_1[N]$ satisfying $4C < N^2$.
2. Set $P' := \mathsf{A}(\mathcal{R}_\sigma, P_1)$, $Q' := \mathsf{A}(\mathcal{R}_\sigma, Q_1)$, where $P', Q' \in E_2[N]$.
3. Set $X := \hat{w}'(P_1)$ and $Y := \hat{w}'(Q_1)$ as unknowns for which we look for the value. Then, X and Y can be written as
$$X = [a]P_\psi + [b]Q_\psi, \qquad Y = [c]P_\psi + [d]Q_\psi,$$
for some unknown values $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$, where $\langle P_\psi, Q_\psi \rangle = E_\psi[N]$.

4. From the action of isogeny $\tilde{\sigma}$ on X and Y, that is,

$$\tilde{\sigma}(X) = \tilde{\sigma}([a]P_\psi + [b]Q_\psi) = [a]\tilde{\sigma}(P_\psi) + [b]\tilde{\sigma}(Q_\psi),$$
$$\tilde{\sigma}(Y) = \tilde{\sigma}([c]P_\psi + [d]Q_\psi) = [c]\tilde{\sigma}(P_\psi) + [d]\tilde{\sigma}(Q_\psi),$$

we form the following equations:

$$[a]\tilde{\sigma}(P_\psi) + [b]\tilde{\sigma}(Q_\psi) = P',$$
$$[c]\tilde{\sigma}(P_\psi) + [d]\tilde{\sigma}(Q_\psi) = Q',$$

where P', Q' have already been obtained from step 2.

5. Set initial values for a and c, (we let $a = c = 1$). Using Discrete Logarithm (DL) algorithm, $\mathcal{A}_{\mathsf{DLP}}$, the values of b and d can be found. This way, the action of $\hat{w'}$ on P_1 and Q_1 is determined.

6. Exploit the SIDH attack, $\mathcal{A}_{\mathsf{SIDH}}$, to find the kernel of the isogeny $\hat{w'}$. Then, compute dual of $\hat{w'}$, that is the isogeny $w' : E_\psi \to E_1$. Let $\ker(w') = \langle [\alpha_1]P'_\psi + [\alpha_2]Q'_\psi \rangle$, for some $\alpha_1, \alpha_2 \in \mathbb{Z}/C\mathbb{Z}$, and $\langle P'_\psi, Q'_\psi \rangle = E_\psi[C]$.

7. Recompute α_1, α_2 by making change of basis $\langle P'_\psi, Q'_\psi \rangle$ into $\langle \psi(P), \psi(Q) \rangle$, and obtain $\alpha \in \mathbb{Z}/C\mathbb{Z}$ for which $\ker(w') = \langle \psi(P) + [\alpha]\psi(Q) \rangle$.

8. Compute pull-back of the isogeny w' through ψ using public parameters P, Q, to extract the witness isogeny $w : E_0 \to E_w := E_0/\langle P + [\alpha]Q \rangle$.

Thus, the extracting algorithm is defined as follows:

$$w \,/\, \perp \leftarrow \mathsf{Ext}(\Sigma, \tilde{\Sigma}, \mathsf{s}) = \mathsf{Ext}\Big((E_1, \mathcal{R}_\sigma), (E_1, \pi_{\psi'}, E_\psi, S, R_{\tilde{\sigma}}), (E_w, w(\mathfrak{B}))\Big).$$

Algorithm 1 $\mathsf{SQIAsignHD}$: Adaptor Signature $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$

Public Parameters. A prime $p = ABCf - 1$, where $A = 2^a$, $B = \prod_{i=1}^{t} \ell_i$, and $C = 3^c$ are pairwise coprime integers, f is some (small) cofactor, ℓ_i's are distinct small primes, $A \approx p^{3/10}$, $B \approx p^{3/5}$, and $C \approx p^{1/10}$. A supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ with $\mathrm{End}(E_0) \cong \mathcal{O}_0 \subset \mathcal{B}_{p,\infty}$, and $|E_0(\mathbb{F}_{p^2})| = (p+1)^2$. An artificial B-orientation $\mathfrak{B} = (G_1, G_2)$ on E_0, and a torsion basis $\langle P, Q \rangle = E_0[C]$.

Procedure $\mathsf{PreSign}(\mathsf{sk}, \mathsf{m}, \mathsf{s})$
    Compute a secret isogeny $\psi : E_0 \to E_\psi$.
    Compute the image of P, Q under ψ, and set $S := (\psi(P), \psi(Q))$.
    Compute the push-forward $\psi' := [w]_* \psi : E_w \to E_1$ via $w(\mathfrak{B})$.
    Compute the zero-knowledge $\pi_{\psi'}$ showing that E_1 is honestly generated.
    Compute $\varphi := \Phi(E_\tau, h) : E_\tau \to E_2$, where $h := \mathsf{H}(j(E_1), m)$.
    Compute $\mathcal{R}_{\tilde{\sigma}} := (\tilde{\sigma}(R_1), \tilde{\sigma}(R_2), \tilde{q})$ where $\tilde{\sigma} : E_\psi \to E_2$ of degree $\tilde{q}$.
    Return $\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

Procedure $\mathsf{PreVer}(\mathsf{pk}, \mathsf{m}, \mathsf{s}, \tilde{\Sigma})$
    Parse $\tilde{\Sigma}$ as $(E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$.
    Check that $e_C(\psi(P), \psi(Q)) = e_C(P, Q)^B$.
    Verify that $1 = \mathsf{NIZK.V}(E_1, \pi_{\psi'})$.
    Compute $h := H(j(E_1), m)$ and recover $\varphi := \Phi(E_\tau, h) : E_\tau \to E_2$.
    Check that $\mathcal{R}_{\tilde{\sigma}}$ correctly represent $\tilde{\sigma} : E_\psi \to E_2$.
    Return $0/1$.

Procedure $\mathsf{Adapt}(\tilde{\Sigma}, \mathsf{w})$
    Compute push-forward $w' := [\psi]_* w : E_\psi \to E_1$ via S.
    Determine a canonical basis $\langle P_0, Q_0 \rangle = E_1[AC]$.
    Compute $\sigma(P_0) := \mathsf{A}(\mathcal{R}_{\tilde{\sigma}}, \hat{w}'(P_0))$, and $\sigma(Q_0) := \mathsf{A}(\mathcal{R}_{\tilde{\sigma}}, \hat{w}'(Q_0))$.
    Set $\mathcal{R}_\sigma := (\sigma(P_0), \sigma(Q_0), q)$ where $\sigma : E_1 \to E_2$, and $q = \deg(\sigma)$.
    Return $\Sigma := (E_1, \mathcal{R}_\sigma)$

Procedure $\mathsf{Ext}(\tilde{\Sigma}, \Sigma, \mathsf{s})$
    Parse Σ as $(E_1, \mathcal{R}_\sigma)$.
    Recover $\hat{w}' : E_1 \to E_\psi$ via $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$.
    Compute $w' : E_\psi \to E_\psi / \langle [\alpha_1] P'_\psi + [\alpha_2] Q'_\psi \rangle$ where $\langle P'_\psi, Q'_\psi \rangle = E_\psi[C]$.
    Recompute α_1, α_2 by changing basis $\langle P'_\psi, Q'_\psi \rangle$ into $\langle \psi(P), \psi(Q) \rangle$.
    Extract w by pulling w' back through ψ via public points P, Q.
    Return $\perp$ / w

4 Security Proof

In this section, we analyze and formally prove the security of the new adaptor signature $\Xi_{\mathsf{R}_{\mathfrak{A}},\Sigma_{\mathsf{SQIsignHD}}}$. We show that $\Xi_{\mathsf{R}_{\mathfrak{A}},\Sigma_{\mathsf{SQIsignHD}}}$ satisfies pre-signature correctness, pre-signature adaptability, aEUF-CMA, and witness extractability properties. Verifying these properties suffices to prove the Theorem 4.11.

Lemma 4.1. *The adaptor signature* $\Xi_{\mathsf{R}_{\mathfrak{A}},\Sigma_{\mathsf{SQIsignHD}}}$ *is pre-signature correct.*

Proof. First, we let $(\mathsf{w},\mathsf{s}) := \big(w,(E_w,w(\mathfrak{B}))\big)$ be a fixed witness/statement pair of the defined hard relation $\mathsf{R}_{\mathfrak{A}}$, generated by the GenR algorithm, where w is an isogeny from E_0 to the target elliptic curve E_w, and $w(\mathfrak{B})$ is the image of B-orientation $\mathfrak{B}$ under the witness isogeny w. Moreover, suppose that $(\mathsf{sk},\mathsf{pk}) := (\tau, E_\tau)$ is a fixed secret/public key pair generated by the KeyGen algorithm.
Assume that for a message $m \in \{0,1\}^*$, the pre-signature $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$ is generated via PreSig algorithm, i.e., $\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big)$. In this case, we necessarily obtain $1 \leftarrow \mathsf{PreVer}(E_\tau, m, E_w, \tilde{\Sigma})$ meaning that $\mathcal{R}_{\tilde{\sigma}}$ is an efficient representation of an isogeny $\tilde{\sigma}$ from E_ψ to E_2, where E_2 is the target curve of isogeny φ depending on the message m and the commitment curve E_1, verified via $1 = \mathsf{NIZK.V}(E_1, \pi_{\psi'})$, which is obtained by pushing-forward the commitment isogeny ψ through witness isogeny w starting at the statement curve $(E_w, w(\mathfrak{B}))$.
Next, the (full) signature $\Sigma = (E_1, \mathcal{R}_\sigma)$ is produced by adaptation algorithm, that is $\Sigma \leftarrow \mathsf{Adapt}(\tilde{\Sigma}, w)$. Here, $\mathcal{R}_\sigma$ is an efficient representation of the signature isogeny σ with domain E_1 and codomain E_2 obtained from the composition of $\hat{w'}$ (the dual of the push-forward of the witness w through ψ using S), i.e., $\sigma := \tilde{\sigma} \circ \widehat{[\psi]_* w} = \tilde{\sigma} \circ \hat{w'} : E_1 \to E_2$. Hence, the verification of the signature can be done by SQIsignHD verifying algorithm Ver necessarily yielding $1 \leftarrow \mathsf{Ver}(E_\tau, m, \mathsf{Adapt}(\tilde{\Sigma}, w))$. It means that the data $\mathcal{R}_\sigma$ represent correctly the signature isogeny σ which is a map from the curve E_1 to E_2.
From the knowledge of the pre-signature $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$ and signature $\Sigma = (E_1, \mathcal{R}_\sigma)$, and using discrete logarithm $\mathcal{A}_{\mathsf{DLP}}$ and SIDH attack $\mathcal{A}_{\mathsf{SIDH}}$, we can extract the $w' : E_\psi \to E_1$ revealing the witness w via its pull-back through the secret isogeny ψ using points $P, Q, \psi(P)$, and $\psi(Q)$. This means that $w \leftarrow \mathsf{Ext}\big(\Sigma, \tilde{\Sigma}, (E_w, w(\mathfrak{B}))\big)$ is successfully performed to obtain the witness w . Thus, the adaptor signature $\Xi_{\mathsf{R}_{\mathfrak{A}},\Sigma_{\mathsf{SQIsignHD}}}$ satisfies the pre-signature correctness property. □

Lemma 4.2. *The adaptor signature* $\Xi_{\mathsf{R}_{\mathfrak{A}},\Sigma_{\mathsf{SQIsignHD}}}$ *is pre-signature adaptable.*

Proof. Let define a fixed witness/statement pair $(\mathsf{w},\mathsf{s}) := \big(w,(E_w,w(\mathfrak{B}))\big) \in \mathsf{R}_{\mathfrak{A}}$, a fixed public key $\mathsf{pk} = E_\tau$, and a pre-signature $\tilde{\Sigma}$, and a message $m \in \{0,1\}^*$ as in the previous Lemma.
We want to prove that any verifiably valid (but, not necessarily honestly generated) pre-signature $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$ passing PreVer algorithm, can be adapted into a valid (full) signature Σ. To show this, let $\mathsf{PreVer}(E_\tau, m, E_w, \tilde{\Sigma}) = 1$ meaning that $\mathsf{NIZK.V}(E_1, \pi_{\psi'}) = 1$, and $\mathcal{R}_{\tilde{\sigma}}$ is a data representing an isogeny from E_ψ to E_2, where E_2 is a target curve of φ generated by the message m and commitment curve E_1. In this case, by using the correctness property as shown in the previous Lemma, the adapting algorithm Adapt necessarily yields a full signature Σ which is verifiable by the verifying

algorithm Ver of the $\Sigma_{\mathsf{SQIsignHD}}$. Finally, the witness $\mathsf{w} = w$ can be extracted by using the valid pre-signature/signature pair and the corresponding statement $\mathsf{s} = (E_w, w(\mathfrak{B}))$, i.e., $w \leftarrow \mathsf{Ext}(\Sigma, \tilde{\Sigma}, \mathsf{s})$. Therefore, the adaptor signature $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ satisfies the pre-signature adaptability property. □

Lemma 4.3. *Let the SQIsignHD signature scheme* $\Sigma_{\mathsf{SQIsignHD}}$ *be* $\mathsf{SUF\text{-}CMA}$ *secure, and let* $\mathsf{R}_{\mathfrak{A}}$ *be a hard relation. Then, the adaptor signature scheme* $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ *is* $\mathsf{aEUF\text{-}CMA}$ *secure in the quantum random oracle model.*

Proof. We start our proof by reducing the SQIAsignHD adaptor signature's unforgeability to the SQIsignHD signature scheme's strong unforgeability. Starting with the $\mathsf{aSigForge}$, we play a series of games with adversary $\mathcal{A}$ in which we can respond to all of $\mathcal{A}$'s query calls, up until the last game in the series. Our initial focus is how to provide $\mathcal{A}$ with the signing and pre-signing queries. If we are successful in responding to these calls, we will be able to leverage its forgery to win our $\mathsf{aSigForge}$ game. In order to achieve this, we construct a simulator $\mathcal{S}$ that employs $\mathcal{A}$'s forgery in $\mathsf{aSigForge}$ to win its strong unforgeability experiment for the SQIsignHD signature scheme. In this case, $\mathcal{S}$ has access to both signing oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ and the random oracle $\mathcal{H}^{\mathsf{SQIsignHD}}$, and it utilizes them to simulate oracle queries for $\mathcal{A}$, namely random oracle $\mathcal{H}$, signing queries $\mathcal{O}_S$, and pre-signing queries $\mathcal{O}_{pS}$. Furthermore, since a valid pre-signature contains a zero-knowledge proof $\pi_{\psi'}$ related to secret parallel isogeny ψ' to isogeny ψ, then the simulator $\mathcal{S}$ has to simulate a proof without knowledge of the corresponding secret isogeny. To do this, we exploit the zero-knowledge property allowing us to simulate a proof for a commitment curve E_1 without knowing the corresponding isogeny.

Game_0. This game corresponds to the $\mathsf{aSigForge}$ experiment given in Definition 2.12, where the adversary $\mathcal{A}$ has access to a random oracle $\mathcal{H}$, in the random oracle model, and many previously produced valid pre-signatures and signatures through pre-signing $\mathcal{O}_{pS}$ and signing oracles $\mathcal{O}_S$ on messages of its choice but a message m, and forges a verifiable signature Σ^* on the message m. Hence, in this setting, it follows that

$$\Pr[\mathsf{Game}_0 = 1] = \Pr[\mathsf{aSigForge}_{\mathcal{A}, \Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}}(\lambda) = 1].$$

Game_1. This game is analogous to the game Game_0. The only difference is that if a valid signature Σ^*, forged by the adversary $\mathcal{A}$, is the same as the output of adaptation of the pre-signature into a signature with the help of the corresponding witness, then the game aborts.

Game_0

```
Q := ∅
H := [⊥]
(τ, E_τ) ← KeyGen(1^λ)
m ← A^{O_S(·), O_pS(·,·)}(E_τ)
(w, (E_w, w(𝔅))) ← GenR(1^λ)
Σ̃ ← PreSig(τ, m, (E_w, w(𝔅)))
Σ* ← A(Σ̃, (E_w, w(𝔅)))
b := Ver(E_τ, m, Σ*)
return m ∉ Q ∧ b
```

$\mathcal{O}_S(m)$

```
Σ ← Sig(τ, m)
Q := Q ∪ {m}
return Σ
```

$\mathcal{H}(x)$

```
if H[x] = ⊥
    H[x] ← H^SQIsignHD(x)
return H[x]
```

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

```
Σ̃ ← PreSig(τ, m, (E_w, w(𝔅)))
Q := Q ∪ {m}
return Σ̃
```

Game_1

```
Q := ∅
H := [⊥]
(τ, E_τ) ← KeyGen(1^λ)
m* ← A^{O_S(·), O_pS(·,·)}(E_τ)
(w, (E_w, w(𝔅))) ← GenR(1^λ)
Σ̃ ← PreSig(τ, m*, (E_w, w(𝔅)))
Σ* ← A(Σ̃, (E_w, w(𝔅)))
if Adapt(Σ̃, w) = Σ*
    abort
b := Ver(E_τ, m*, Σ*)
return m* ∉ Q ∧ b
```

$\mathcal{O}_S(m)$

```
Σ ← Sig(τ, m)
Q := Q ∪ {m}
return Σ
```

$\mathcal{H}(x)$

```
if H[x] = ⊥
    H[x] ← H^SQIsignHD(x)
return H[x]
```

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

```
Σ̃ ← PreSig(τ, m, (E_w, w(𝔅)))
Q := Q ∪ {m}
return Σ̃
```

Claim 4.4. *If* Bad_1 *is the event that* Game_1 *aborts, then we claim that for a negligible function* negl *in* λ*,* $Pr[\mathsf{Bad}_1] \leq \mathsf{negl}(\lambda)$*.*

Proof. The claim is proven by a reduction to the hardness of the relation $\mathsf{R}_{\mathfrak{A}}$. To do this, we construct a simulator $\mathcal{S}$ breaking the hardness of $\mathsf{R}_{\mathfrak{A}}$ and assuming that it has access to an adversary $\mathcal{A}$ that causes Game_1 to abort with the non-negligible probability. The simulator receives a challenge $\mathsf{s}^* = (E_w, w(\mathfrak{B}))^*$, and generates a secret/public key pair $(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$ to simulate $\mathcal{A}$'s queries to the oracles $\mathcal{H}$, $\mathcal{O}_{pS}$ and $\mathcal{O}_S$. The functionalities of the simulated oracles are as described in Game_1. Based on receiving the challenge message m^* from $\mathcal{A}$, $\mathcal{S}$ computes a pre-signature $\tilde{\Sigma} \leftarrow \mathsf{PreSig}(\tau, m^*, (E_w, w(\mathfrak{B}))^*)$ and returns the pair $(\tilde{\Sigma}, (E_w, w(\mathfrak{B}))^*)$ to the adversary who forges a signature by using the returned pair. Assuming that Bad_1 happened (i.e., $\mathsf{Adapt}(\tilde{\Sigma}, w) = \Sigma^*$), since the $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ is pre-signature correct as in Definition 2.10, the simulator can extract w^* via $\mathsf{Ext}(\Sigma^*, \tilde{\Sigma}, (E_w, w(\mathfrak{B}))^*)$ to obtain a valid witness/statement pair such that $(w^*, (E_w, w(\mathfrak{B}))^*) \in \mathsf{R}_{\mathfrak{A}}$, thereby $\mathcal{S}$ breaks the security of the relation $\mathsf{R}_{\mathfrak{A}}$. We note that the view of $\mathcal{A}$ in this simulation and Game_1 are indistinguishable since the challenge $(E_w, w(\mathfrak{B}))^*$ is an instance of the hard relation $\mathsf{R}_{\mathfrak{A}}$ and has the same distribution to the public output of GenR. Therefore, the probability that $\mathcal{S}$ breaks the hardness of $\mathsf{R}_{\mathfrak{A}}$ is equal to the probability that the event Bad_1 happens that is non-negligible by assumption. This contradicts the hardness of $\mathsf{R}_{\mathfrak{A}}$. Since Game_1 and Game_0 are equivalent except in case of happening the event Bad_1, it follows that

$$\Pr[\mathsf{Game}_1 = 1] \leq \Pr[\mathsf{Game}_0 = 1] + \mathsf{negl}(\lambda).$$

□

Game_2. This game is analogous to the previous game. The only difference is a modification in the pre-signing oracle $\mathcal{O}_{pS}$. That is, in this game we apply the online extractor algorithm $\mathcal{E}$ taking the statement $(E_w, w(\mathfrak{B}))$, and the list of random oracle queries H as input to extract a witness w through the $\mathcal{O}_{pS}$ queries. The game aborts in case $\big(w, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$ for the extracted witness w.

Claim 4.5. *If* Bad_2 *is the event that* Game_2 *aborts during an* $\mathcal{O}_{pS}$ *execution, then* $Pr[\mathsf{Bad}_2] \leq \mathsf{negl}(\lambda)$ *for a negligible function* negl *in* λ*.*

Proof. In the quantum random oracle model, the oracle can extract the witness using its online extractor algorithm $\mathcal{E}$. More precisely, there is a non-negligible probability that $\big(w, (E_w, w(\mathfrak{B}))\big) \in \mathsf{R}_{\mathfrak{A}}$, where $w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$. □

Since games Game_2 and Game_1 are equivalent except in case Bad_2 happens, it follows that

$$Pr[\mathsf{Game}_2 = 1] \leq Pr[\mathsf{Game}_1 = 1] + \mathsf{negl}(\lambda).$$

Game_2

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\big(w, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathsf{GenR}(1^\lambda)$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m^*, (E_w, w(\mathfrak{B}))\big)$
$\Sigma^* \leftarrow \mathcal{A}\big(\tilde{\Sigma}, (E_w, w(\mathfrak{B}))\big)$
if $\mathsf{Adapt}(\tilde{\Sigma}, w) = \Sigma^*$
  abort
$b := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
return $m^* \notin \mathcal{Q} \wedge b$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \bot$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w^* := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $\big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma}$

Game_3

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\big(w, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathsf{GenR}(1^\lambda)$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m^*, (E_w, w(\mathfrak{B}))\big)$
$\Sigma^* \leftarrow \mathcal{A}\big(\tilde{\Sigma}, (E_w, w(\mathfrak{B}))\big)$
if $\mathsf{Adapt}(\tilde{\Sigma}, w) = \Sigma^*$
  abort
$b := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
return $m^* \notin \mathcal{Q} \wedge b$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \bot$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w^* := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w^*, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

Game_3. In this game, we apply further modifications to the pre-signing oracle $\mathcal{O}_{pS}$ to create a correct pre-signature $\tilde{\Sigma}$. First, by executing the Sig algorithm, the signature Σ is produced. Then, with the help of the signature Σ, the witness w which has been already extracted from the online extractor $\mathcal{E}$, and zero-knowledge proof $\pi_{\psi'}$ which can be simulated computationally indistinguishable by the simulator due to the zero-knowledge property of NIZK, the pre-signature is created. We see that this game is indistinguishable from the previous game, and it follows that

$$Pr[\mathsf{Game}_3 = 1] \le Pr[\mathsf{Game}_2 = 1] + \mathsf{negl}(\lambda).$$

Game_4. In this game, after receiving the challenge message m^* from $\mathcal{A}$, as in the previous game during the $\mathcal{O}_{pS}$ execution, the game generates a signature Σ by running the Sig algorithm and converting the resulting signature into a valid pre-signature. Therefore, in this game as well, the same indistinguishability argument that held in the previous game holds. Thus, it follows that

$$Pr[\mathsf{Game}_4 = 1] \le Pr[\mathsf{Game}_3 = 1] + \mathsf{negl}(\lambda).$$

Game_4

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\big(w, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathsf{GenR}(1^\lambda)$
$\Sigma \leftarrow \mathsf{Sig}(\tau, m^*)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$
$\Sigma^* \leftarrow \mathcal{A}\big(\tilde{\Sigma}, (E_w, w(\mathfrak{B}))\big)$
if $\mathsf{Adapt}(\tilde{\Sigma}, w) = \Sigma^*$
  abort
$b := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
return $m^* \notin \mathcal{Q} \wedge b$

$\mathcal{H}(x)$

if $H[x] = \perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w^* := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w^*, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

As it can be seen, the transformation of the $\mathsf{aSigForge}$ game into game Game_4 is indistinguishable. Thus, the original $\mathsf{aSigForge}$ game has now been reduced to Game_4, a game in which we are able to respond to $\mathcal{A}$'s query calls. More precisely, if the adversary $\mathcal{A}$ queries the signing oracle $\mathcal{O}_S$, the simulator $\mathcal{S}$ queries the SQIsignHD signing oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ and returns its response to $\mathcal{A}$. In case $\mathcal{A}$ queries the pre-signing oracle, the simulator, first, extracts w using the online extractability of NIZK, then queries the SQIsignHD signing oracle to get the signature, finally uses the signature, the resulting witness, the simulated proof $\pi_{\psi'}$ to create a valid pre-signature. Moreover, based on $\mathcal{A}$ querying the oracle $\mathcal{H}$ on input x, in case $H[x] =\perp$, the $\mathcal{S}$ queries $\mathcal{H}^{\mathsf{SQIsignHD}}(x)$, otherwise the simulator outputs $H[x]$. Thus, adversary $\mathcal{A}$ is able to make any queries to the oracles it requires, thereby generating a forgery. The only thing remaining to show is that there exists a simulator that simulates Game_4 and utilizes the resulting forgery due to $\mathcal{A}$ to win the SQIsignHD $\mathsf{SigForge}$ game or the $\mathsf{StrongSigForge}$ game.

$\mathcal{S}^{\mathsf{Sig}^{\mathsf{SQIsignHD}},\mathcal{H}^{\mathsf{SQIsignHD}}}(E_\tau)$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\big(w, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathsf{GenR}(1^\lambda)$
$\boldsymbol{\Sigma} \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m^*)$
Parse $\boldsymbol{\Sigma}$ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\tilde{\boldsymbol{\Sigma}} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$
$\boldsymbol{\Sigma}^* \leftarrow \mathcal{A}\big(\tilde{\boldsymbol{\Sigma}}, (E_w, w(\mathfrak{B}))\big)$
return $(m^*, \boldsymbol{\Sigma}^*)$

$\mathcal{O}_S(m)$

$\boldsymbol{\Sigma} \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\boldsymbol{\Sigma}$

$\mathcal{H}(x)$

if $H[x] =\perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w^* := \mathcal{E}(E_w, \pi_w, H)$
if $(w^*, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\boldsymbol{\Sigma} \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m)$
Parse $\boldsymbol{\Sigma}$ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\boldsymbol{\Sigma}} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

Claim 4.6. $(m^*, \boldsymbol{\Sigma}^*)$ *constitutes a valid forgery in the* $\mathsf{StrongSigForge}$ *game.*

Proof. To prove this claim, we must show that the pair $(m^*, \boldsymbol{\Sigma}^*)$ has not been output by the oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ before. Note that the adversary $\mathcal{A}$ has not previously made a query on the challenge message m^* to either $\mathcal{O}_S$ or $\mathcal{O}_{pS}$. Therefore, $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ is only queried on m^* during the challenge phase. As shown in the game Game_1, the adversary outputs a forgery Σ^* which is equal to the signature Σ output by $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ during the challenge phase only with negligible probability. Hence, oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ has never output Σ^* on query m^* before, and thus (m^*, Σ^*) is a valid forgery for the $\mathsf{StrongSigForge}$ game. □

From the game Game_0 to the game Game_4, we have that

$$\Pr[\mathsf{Game}_0 = 1] \leq \Pr[\mathsf{Game}_4 = 1] + \mathsf{negl}(\lambda).$$

Due to a perfect simulation of Game_4, provided by the simulator $\mathcal{S}$, it follows that

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{aSigForge}} = \Pr[\mathsf{Game}_0 = 1] \leq \Pr[\mathsf{Game}_4 = 1] + \mathsf{negl}(\lambda) \leq \mathsf{Adv}_{\mathcal{S}}^{\mathsf{StrongSigForge}} + \mathsf{negl}(\lambda).$$

By assumption, as SQIsignHD is secure in QROM with $\mathcal{H}^{\mathsf{SQIsignHD}}$ programmed as a quantum random oracle, it implies that our adaptor signature, $\mathsf{SQIAsignHD}$, is $\mathsf{aEUF\text{-}CMA}$ secure in QROM. □

Lemma 4.7. *Let the SQIsignHD signature scheme $\Sigma_{\mathsf{SQIsignHD}}$ be $\mathsf{SUF\text{-}CMA}$, and $\mathsf{R}_{\mathfrak{A}}$ be a hard relation. Then, the adaptor signature $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ is witness extractable in the quantum random oracle model.*

Proof. The proof of this lemma is almost identical to the proof of Lemma 4.3. We prove this lemma by reducing the witness extractability of $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ to the strong unforgeability of the SQIsignHD signature scheme. More precisely, let $\mathcal{A}$ be a PPT adversary who wins the $\mathsf{aWitExt}$ game, then we build another PPT adversary $\mathcal{S}$ so that it wins the $\mathsf{StrongSigForge}$ game.
Analogous to the proof of the previous Lemma, the main challenge comes from the simulation of pre-signing queries. The difference now from the previous Lemma is that in $\mathsf{aWitExt}$, the adversary $\mathcal{A}$ outputs the statement $(E_w, w(\mathfrak{B}))$ for the relation $\mathsf{R}_{\mathfrak{A}}$ along with the challenge message m^*. This means that the pair $\big(w, (E_w, w(\mathfrak{B}))\big)$ is not chosen by the game. Consequently, $\mathcal{S}$ is unable to convert a valid signature into a pre-signature as it does not have access to the witness w. However, w can be extracted by the online extractor $\mathcal{E}$ since we are in the QROM. Once w is extracted, then S can simulate the pre-signing queries as in the previous Lemma. We, now, begin with designing a series of games required for the proof.

Game_0. This game is the $\mathsf{aWitExt}$ game given in Definition 2.13. For a given pre-signature $\tilde{\Sigma}$ and witness/statement pair $\big(w, (E_w, w(\mathfrak{B}))\big)$, the adversary $\mathcal{A}$ who has access to oracles $\mathcal{H}$, $\mathcal{O}_{pS}$ and $\mathcal{O}_S$, needs to generate a valid signature Σ for a message m of its choice such that $\big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$, where $w^* = \mathsf{Ext}(\tilde{\Sigma}, \Sigma, (E_w, w(\mathfrak{B})))$. Since Game_0 is exactly the $\mathsf{aWitExt}$ game, then we have

$$\Pr[\mathsf{Game}_0 = 1] = \Pr[\mathsf{aWitExt}_{\mathcal{A}, \Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}}(\lambda) = 1].$$

Game_0

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big)$
$\Sigma \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
$w^* := \mathsf{Ext}\big(\tilde{\Sigma}, \Sigma, (E_w, w(\mathfrak{B}))\big)$
$b_1 := \mathsf{Ver}(E_\tau, m, \Sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := \big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
$\textbf{return } b_1 \wedge b_2 \wedge b_3$

$\mathcal{H}(x)$

$\textbf{if } H[x] = \perp$
$\quad H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
$\textbf{return } H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
$\textbf{return } \tilde{\Sigma}$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
$\textbf{return } \Sigma$

Game_1

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m^*, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\mathsf{sk}, m^*, (E_w, w(\mathfrak{B}))\big)$
$\Sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
$w^* := \mathsf{Ext}\big(\tilde{\Sigma}, \Sigma^*, (E_w, w(\mathfrak{B}))\big)$
$b_1 := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := \big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
$\textbf{return } b_1 \wedge b_2 \wedge b_3$

$\mathcal{H}(x)$

$\textbf{if } H[x] = \perp$
$\quad H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
$\textbf{return } H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
$\textbf{if } (w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
$\quad \textbf{abort}$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m, (E_w, w(\mathfrak{B}))\big)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
$\textbf{return } \tilde{\Sigma}$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
$\textbf{return } \Sigma$

Game_1. This game is the same as Game_0 except that some changes is applied to the pre-signing oracle $\mathcal{O}_{pS}$. More precisely, during the $\mathcal{O}_{pS}$ queries, this game extracts a witness w by executing the online extractor algorithm $\mathcal{E}$ on inputs which are the statement $(E_w, w(\mathfrak{B}))$ and the list of random oracle queries H. The game aborts in case for the extracted witness w, $\big(w, (E_w, w(\mathfrak{B}))\big) \in \mathsf{R}_{\mathfrak{A}}$ is not satisfied.

Claim 4.8. *If* Bad_1 *is the event that* Game_1 *aborts while the execution of* $\mathcal{O}_{pS}$*, then* $Pr[\mathsf{Bad}_1] \leq \mathsf{negl}(\lambda)$.

Proof. From the online extractor property of NIZK, the witness w can be extracted via the extractor $\mathcal{E}$ for which $\big(w, (E_w, w(\mathfrak{B}))\big) \in \mathsf{R}_{\mathfrak{A}}$ is satisfied except with negligible probability. □

It follows that Game_1 and Game_0 are equivalent except for the case that the event Bad_1 happens. Thus, we get that

$$\Pr[\mathsf{Game}_0 = 1] \leq \Pr[\mathsf{Game}_1 = 1] + \mathsf{negl}(\lambda).$$

Game_2. We apply further modifications to the $\mathcal{O}_{pS}$ oracle from the previous game. In this game, first a valid full signature Σ is created by executing the Sig algorithm and converted Σ into a pre-signature by using the extracted witness w obtained from the online extractor $\mathcal{E}$, and proof $\pi_{\psi'}$ which is generated by the simulator $\mathcal{S}$. We see that this game is indistinguishable from the previous game, and it follows that

$$\Pr[\mathsf{Game}_1 = 1] \leq \Pr[\mathsf{Game}_2 = 1] + \mathsf{negl}(\lambda).$$

Game_2

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m^*, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m^*, (E_w, w(\mathfrak{B}))\big)$
$\Sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
$w^* := \mathsf{Ext}\big(\tilde{\Sigma}, \Sigma^*, (E_w, w(\mathfrak{B}))\big)$
$b_1 := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := \big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
return $b_1 \wedge b_2 \wedge b_3$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} := (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

Game_3

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m^*, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\tilde{\Sigma} \leftarrow \mathsf{PreSig}\big(\tau, m^*, (E_w, w(\mathfrak{B}))\big)$
$\Sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
$w^* := \mathsf{Ext}\big(\tilde{\Sigma}, \Sigma^*, (E_w, w(\mathfrak{B}))\big)$
$b_1 := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := \big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
return $b_1 \wedge b_2 \wedge b_3$

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

Game_3. In this game, for the challenge phase, we apply the identical modifications implemented in Game_1's $\mathcal{O}_{pS}$ oracle. In the challenge phase, a witness w is extracted by the online extractor algorithm $\mathcal{E}$ taking the statement $(E_w, w(\mathfrak{B}))$, and the list of random oracle queries H as inputs. In case for the extracted witness w, the relation $\big(w, (E_w, w(\mathfrak{B}))\big) \in \mathsf{R}_{\mathfrak{A}}$ is not satisfied, then the game aborts.

Claim 4.9. *If* Bad_2 *is the event that* Game_3 *aborts during the challenge phase, then* $Pr[\mathsf{Bad}_2] \leq \mathsf{negl}(\lambda)$.

Proof. The same arguments in Claim 4.8 hold for proving this claim. □

Hence, Game_3 and Game_2 are equivalent except for the case that the event Bad_2 happens. Thus, we have

$$\Pr[\mathsf{Game}_2 = 1] \leq \Pr[\mathsf{Game}_3 = 1] + \mathsf{negl}(\lambda).$$

Game_4. The challenge phase of this game uses the similar modifications implemented in Game_2 for the $\mathcal{O}_{pS}$ oracle. That is, using the extracted witness w, this game first uses the Sig algorithm to construct a valid full signature Σ, which it then transforms into a pre-signature with the help of the online extractor $\mathcal{E}$ and the zero-knowledge proof simulator $\mathcal{S}$. Hence, this game is indistinguishable from the previous game, and it follows that

$$\Pr[\mathsf{Game}_3 = 1] \leq \Pr[\mathsf{Game}_4 = 1] + \mathsf{negl}(\lambda).$$

After demonstrating that the transformation of original $\mathsf{aWitExt}$ game into Game Game_4 is indistinguishable, it is necessary to show that there exists a simulator that accurately simulates Game_4 and utilizes the adversary $\mathcal{A}$ to win the $\mathsf{StrongSigForge}$ game.

Game_4

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m^*, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_\mathfrak{A}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$
$\Sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
$w^* := \mathsf{Ext}\big(\tilde{\Sigma}, \Sigma^*, (E_w, w(\mathfrak{B}))\big)$
$b_1 := \mathsf{Ver}(E_\tau, m^*, \Sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := \big(w^*, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_\mathfrak{A}$
return $b_1 \wedge b_2 \wedge b_3$

$\mathcal{O}_S\big(m\big)$

$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_\mathfrak{A}$
  abort
$\Sigma \leftarrow \mathsf{Sig}(\tau, m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

In the internal mechanism of the simulator S, in case the adversary $\mathcal{A}$ queries the signing oracle $\mathcal{O}_S$ on input m, then the simulator $\mathcal{S}$ will query the SQIsignHD signing oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ and returns its response to the adversary $\mathcal{A}$. In case $\mathcal{A}$ queries the pre-signing oracle on input $\big(m, (E_w, w(\mathfrak{B}))\big)$, first the simulator extracts witness w using the extractability property of NIZK, then queries the SQIsignHD signing oracle on input m to get the signature, finally uses the signature, the corresponding witness, and simulated proof $\pi_{\psi'}$ to construct a valid pre-signature. Moreover, upon $\mathcal{A}$ querying the

$\mathcal{S}^{\mathsf{Sig}^{\mathsf{SQIsignHD}}, \mathcal{H}^{\mathsf{SQIsignHD}}}(E_\tau)$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(\tau, E_\tau) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$\big(m^*, (E_w, w(\mathfrak{B}))\big) \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(E_\tau)$
$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $(w, (E_w, w(\mathfrak{B}))) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m^*)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$
$\Sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\tilde{\Sigma})$
return (m^*, Σ^*)

$\mathcal{O}_S(m)$

$\Sigma \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return Σ

$\mathcal{H}(x)$

if $H[x] = \perp$
  $H[x] \leftarrow \mathcal{H}^{\mathsf{SQIsignHD}}(x)$
return $H[x]$

$\mathcal{O}_{pS}\big(m, (E_w, w(\mathfrak{B}))\big)$

$w := \mathcal{E}(E_w, w(\mathfrak{B}), H)$
if $\big(w, (E_w, w(\mathfrak{B}))\big) \notin \mathsf{R}_{\mathfrak{A}}$
  abort
$\Sigma \leftarrow \mathsf{Sig}^{\mathsf{SQIsignHD}}(m)$
Parse Σ as $(E_1, \mathcal{R}_\sigma)$
Extract $\mathcal{R}_{\tilde{\sigma}}$ by
  $\mathcal{A}_{\mathsf{DLP}}$ and $\mathcal{A}_{\mathsf{SIDH}}$
$\pi_{\psi'} \leftarrow \mathcal{S}(E_1, 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\Sigma} = (E_1, \pi_{\psi'}, E_\psi, S, \mathcal{R}_{\tilde{\sigma}})$

oracle $\mathcal{H}$ on input x, in case $H[x] = \perp$, then $\mathcal{S}$ will query $\mathcal{H}^{\mathsf{SQIsignHD}}(x)$, otherwise the simulator outputs $H[x]$. Therefore, adversary $\mathcal{A}$ can make any queries to the oracles it needs during forgery. Finally, In the challenge phase, after $\mathcal{A}$ creates the message $\big(m, (E_w, w(\mathfrak{B}))\big)$ as the challenge message, the $\mathcal{S}$ uses NIZK's extractability to extract witness w, and sends the message m to the oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ and receives the resulting signature Σ to transform it into a pre-signature. Ultimately, based on forgery made by $\mathcal{A}$, the simulator $\mathcal{S}$ outputs the forgery (m^*, Σ^*).

We end up the proof by showing that there exists a simulator that simulates Game_4 and utilizes the resulting forgery made by $\mathcal{A}$ to win the $\mathsf{StrongSigForge}$ game.

Claim 4.10. (m^*, Σ^*) *constitutes a valid forgery in the* $\mathsf{StrongSigForge}$ *game.*

Proof. It is enough to show that the pair (m^*, Σ^*) has not been created by the oracle $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ before. We note that neither $\mathcal{O}_{pS}$ nor $\mathcal{O}_S$ has received a query from adversary $\mathcal{A}$ regarding the challenge message m^*. $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ is therefore only queried on m^* during the challenge phase. In case the adversary $\mathcal{A}$ creates a forgery Σ^* equal to the signature Σ due to $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ during the challenge phase, then the extracted w would be in relation with the corresponding statement $(E_w, w(\mathfrak{B}))$. Hence, Σ^* on query m^*

has been never output by the $\mathsf{Sig}^{\mathsf{SQIsignHD}}$ before. Thus, (m^*, Σ^*) constitutes a valid forgery for the $\mathsf{StrongSigForge}$ game. $\square$

From the Game_0 to the Game_4, we get that

$$\Pr[\mathsf{Game}_0 = 1] \leq \Pr[\mathsf{Game}_4 = 1] + \mathsf{negl}(\lambda).$$

Since $\mathcal{S}$ provides a perfect simulation of Game_4, we obtain

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{aWitExt}} = \Pr[\mathsf{Game}_0 = 1] \leq \Pr[\mathsf{Game}_4 = 1] + \mathsf{negl}(\lambda) \leq \mathsf{Adv}_{\mathcal{S}}^{\mathsf{StrongSigForge}} + \mathsf{negl}(\lambda).$$

Since SQIsignHD is secure in QROM with $\mathcal{H}^{\mathsf{SQIsignHD}}$ modeled as a quantum random oracle, this implies that the $\mathsf{SQIAsignHD}$ adaptor signature scheme $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ achieves witness extractability even against quantum adversaries. $\square$

Theorem 4.11. *If the SQIsignHD signature scheme,* $\Sigma_{\mathsf{SQIsignHD}}$*, is* $\mathsf{SUF\text{-}CMA}$*, and* $\mathsf{R}_{\mathfrak{A}}$ *is a hard relation, then the* $\mathsf{SQIAsignHD}$ *adaptor signature scheme is secure in quantum random oracle model (QROM).*

Proof. Due to the previous Lemmas of this section, we have shown that the adaptor signature $\Xi_{\mathsf{R}_{\mathfrak{A}}, \Sigma_{\mathsf{SQIsignHD}}}$ satisfies pre-signature correctness, pre-signature adaptability, $\mathsf{aEUF\text{-}CMA}$, and witness extractability properties. Verifying these properties completes the proof of the theorem. $\square$

Conclusion

Adaptor signatures, which are a generalization of standard digital signatures, are a crucial cryptographic primitive for blockchain applications in reducing costs, improving fungibility, and supporting off-chain payment in payment-channel networks and hubs. In the present work, we have introduced $\mathsf{SQIAsignHD}$, a new adaptor signature construction with quantum-resistant security based on isogenies of supersingular elliptic curves. Thereby, it provides security and privacy concepts relevant to off-chain applications. In $\mathsf{SQIAsignHD}$, we use SQIsignHD as the underlying signature scheme and make use of the idea of artificial orientation, on the supersingular isogeny Diffie-Hellman key exchange protocol (SIDH), to apply the hard relation. We also exploit the SIDH attacks as a generic algorithm in recovering the secret witness isogeny in the extraction phase of our scheme. The signature in $\mathsf{SQIAsignHD}$ is approximately 1.5KB in size for $\lambda = 128$ security level. In contrast to the only isogeny-based adaptor signature construction, IAS, which operates on a maximum of the CSIDH-512 parameters, our scheme scales well to high-security levels. Thus, compared to IAS, $\mathsf{SQIAsignHD}$ significantly improves the security level and signature size. Providing a concrete and optimized implementation of $\mathsf{SQIAsignHD}$ is left for future work.

References

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

[2] Poelstra, A.: Scriptless scripts. https://tinyurl.com/ludcxyz (2017)

[3] Aumayr, L., Ersoy, O., Erwig, A., Faust, S., Hostakova, K., Maffei, M., Moreno-Sanchez, P., Riahi, S.: Generalized bitcoin-compatible channels (2020)

[4] Fournier, L.: One-time verifiably encrypted signatures aka adaptor signatures (2019)

[5] Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., Maffei, M.: Anonymous Multi-hop Locks for Blockchain Scalability and Interoperability. Cryptology ePrint Archive (2018)

[6] Moreno-Sanchez, P., Blue, A., Le, D.V., Noether, S., Goodell, B., Kate, A.: DLSAG: Non-interactive refund transactions for interoperable payment channels in Monero. In: Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24, pp. 325–345. Springer (2020)

[7] Tairi, E., Moreno-Sanchez, P., Maffei, M.: A^2L: Anonymous atomic locks for scalability in payment channel hubs. In: 2021 IEEE Symposium on Security and Privacy (SP), pp. 1834–1851. IEEE (2021)

[8] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE (1994)

[9] Esgin, M.F., Ersoy, O., Erkin, Z.: Post-quantum adaptor signatures and payment channel networks. In: European Symposium on Research in Computer Security, pp. 378–397. Springer (2020)

[10] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-Dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238–268. (2018)

[11] Esgin, M.F., Nguyen, N.K., Seiler, G.: Practical exact proofs from lattices: New techniques to exploit fully-splitting rings. 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 26, pp. 259–288. Springer (2020)

[12] Gilchrist, V.: An isogeny-based adaptor signature using SQISign. Master's thesis. http://hdl.handle.net/10012/18157 (2022)

[13] De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: compact post-quantum signatures from quaternions and isogenies. Cryptology ePrint Archive, Paper 2020/1240. https://eprint.iacr.org/2020/1240 (2020)

[14] De Feo, L., Jao, D., Plût, J.: Towards quantum resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Paper 2011/506. https://eprint.iacr.org/2011/506 (2011)

[15] Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 423–447. Springer (2023)

[16] Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 448–471. Springer (2023)

[17] Robert, D.: Breaking SIDH in polynomial time. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 472–503. Springer (2023)

[18] Tairi, E., Moreno-Sanchez, P., Maffei, M.: Post-quantum adaptor signature for privacy-preserving off-chain payments. Cryptology ePrint Archive (2020)

[19] 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)

[20] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An Efficient Post-Quantum Commutative Group Action. Cryptology ePrint Archive, Paper 2018/383. https://eprint.iacr.org/2018/383 (2018)

[21] Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30, pp. 493–522. Springer (2020)

[22] Peikert, C.: He gives C-sieves on the CSIDH. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 463-492. Springer (2020)

[23] De Feo, L., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S., Panny, L., Wesolowski, B.: SCALLOP: scaling the CSI-FiSh. In: IACR International Conference on Public-Key Cryptography, pp. 345–375. Springer (2023)

[24] Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. Cryptology ePrint Archive (2023)

[25] Erwig, A., Faust, S., Hostáková, K., Maitra, M., Riahi, S.: Two-party adaptor signatures from identification schemes. In: Public-Key Cryptography–PKC 2021: 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10–13, 2021, Proceedings, Part I, pp. 451–480. Springer (2021)

[26] Silverman, J.H.: The Arithmetic of Elliptic Curves vol. 106. Springer (2009)

[27] Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendus de l'Académie des Sciences 273, pp. 238–241. (1971)

[28] Kohel, D.R.: Endomorphism rings of elliptic curves over finite fields. Ph.D. thesis, University of California, Berkeley. (1996)

[29] Pizer, A.K.: Ramanujan graphs and Hecke operators. Bulletin (New Series) of the American Mathematical Society 23(1), pp. 127–137. (1990)

[30] Deuring, M.: Die typen der multiplikatorenringe elliptischer funktionenkörper. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 14, pp. 197–272. (1941)

[31] Basso, A., Fouotsa, T.B.: New SIDH countermeasures for a more efficient key exchange. Cryptology ePrint Archive (2023)

[32] Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. Cryptology ePrint Archive, Paper 2020/985. https://eprint.iacr.org/2020/985 (2020)