Π-signHD: A New Structure for the SQIsign Family with Flexible Applicability

Kaizhan Lin[1], Weize Wang[2], Chang-An Zhao[1,3], and Yunlei Zhao✉[2,4]

[1] School of Mathematics, Sun Yat-sen University, Guangzhou, China
linkzh5@mail2.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn
[2] School of Computer Science, Fudan University, Shanghai, China
wzwang23@m.fudan.edu.cn
ylzhao@fudan.edu.cn
[3] Guangdong Key Laboratory of Information Security, Guangzhou, China
[4] State Key Laboratory of Cryptology, Beijing

Abstract. Digital signature is a fundamental cryptographic primitive and is widely used in the real world. Unfortunately, the current digital signature standards like EC-DSA and RSA are not quantum-resistant. Among post-quantum cryptography (PQC), isogeny-based signatures preserve some advantages of elliptic curve cryptosystems, particularly offering small signature sizes. Currently, SQIsign and its variants are the most promising isogeny-based digital signature schemes.

In this paper, we propose a new structure for the SQIsign family: ***P**entagon **I**sogeny-based **Sign**ature in **H**igh **D**imension* (referred to as *Π*-signHD). The new structure separates the hash of the commitment and that of the message by employing two cryptographic hash functions. This feature is desirable in reality, particularly for applications based on mobile low-power devices or for those deployed interactively over the Internet or in the cloud computing setting. This structure can be generally applicable to all the variants of SQIsign. In this work, we focus on the instance based on SQIsignHD, proposed by Dartois, Leroux, Robert and Wesolowski (Eurocrypt 2024). Compared with SQIsignHD, *Π*-signHD has the same signature size (even smaller for some application scenarios). For the NIST-I security level, the signature size of *Π*-signHD can be reduced to 519 bits, while the SQIsignHD signature takes 870 bits. Additionally, *Π*-signHD has an efficient online signing process, and enjoys much desirable application flexibility. In our experiments, the online signing process of *Π*-signHD runs in 4 ms.

Keywords: Digital signatures · SQIsign · SQIsignHD · Isogeny · *Γ*-protocol.

1 Introduction

Isogeny-based cryptography is attractive for its compact keys in post-quantum cryptography, but the expensive computational cost of isogeny computations limits the practical applications of isogeny-based cryptosystems. Various digital signatures under isogeny assumptions have been proposed in recent years, such as [23,13,4,19]. Nevertheless, many of these schemes suffer from relatively large signature or public-key sizes. Conversely, SQIsign [14] and SQIsignHD [12] fully highlight the compactness as isogeny-based signatures.

SQIsign was first introduced by De Feo, Kohel, Leroux, Petit and Wesolowski. SQIsign has a very efficient verification, but the signing phase is expensive due to the ideal-to-isogeny translation, i.e., converting the response ideal to a representation of the corresponding isogeny. Although the ideal-to-isogeny translation has been improved recently [15,25,29], it remains the main efficiency bottleneck in the signing phase. SQIsignHD was proposed by Dartois, Leroux, Robert and Wesolowski. SQIsignHD applies the algorithms derived from SIDH attacks [6,27,33], and offers a remarkably smaller signature size and much faster response since the prover does not need to compute large degree isogenies. Conversely, the verification in SQIsignHD is inefficient as it involves isogeny computations in high dimension.

Motivation. Currently, both SQIsign and SQIsignHD are based on Σ-protocols. Therefore, the challenge is derived from the knowledge of the commitment and the message. However, this feature may result in inconvenient deployments or inefficient implementations, particularly for applications based on low-power devices or applications in the cloud computing setting. We present and discuss some motivating application scenarios below.

- **Application 1: Hardware wallet based on SIM card**. This is a typical application scenario based on mobile low-power devices. In this scenario, the SIM card acts as the signer who keeps the signing secret key and performs signing operations related to the secret key, while the message data (e.g., the payment data) to be signed is usually generated by applications in the mobile phone. When generating a signature based on a Σ-protocol, the SIM card has to compute the hash value of the concatenation of the commitment and the message data (note that when the message data is large, this would be unfriendly as the interaction cost is expensive), or transfer the commitment to the system on chip (SoC) to compute the hash value.
- **Application 2: Document online signing by enterprise**. When using the signature scheme in practice, particularly by enterprises, the signing server is usually deployed in the cloud or run by the enterprise. In this scenario of online signing, Σ-based signatures require the signer to upload the entire document to the signature server. This may consume a significant amount of bandwidth and cause more computing burden on the signature server, resulting in a system bottleneck.

In 1989, Even, Goldreich and Micali [20] introduced online/offline signatures, which are desirable for low-power devices, such as smart cards, sensors, mobile computing processors, and embedded devices. The main idea of online/offline signatures is to divide the signature into the online phase and the offline phase. Generally, the online phase are required to be fast as possible, while the offline phase can be connected to the power. With precomputation in the offline phase, the prover responds in a limited time using a low-power device. In 2013, Yao et al. [38] proposed Γ-protocols and a novel transformation method, known as Γ-transformation. Unlike the signatures based on Σ-protocols and Fiat-Shamir transformation, the signatures via Γ-transformation separate the hash of the commitment a and that of the message m, by employing two secure hash functions h_1 and h_2 to compute the hash values $h_1(a)$ and $h_2(m)$, respectively. From the target one-way property of h_1, the value $h_1(a)$ (or a set of values $\{h_1(a_1), h_1(a_2), \cdots, h_1(a_s)\}$ with commitments a_1, a_2, $\cdots$, a_m) can be public or stored on the verifier's side. Consequently, the verifier can precompute some intermediate values that are relevant to the hash values of the commitment to enhance the verification performance. Moreover, Γ-protocols allow the verifier to compute $h_2(m)$ in advance without the knowledge of the commitment a. When a trusted verifier would like to request the prover to sign a message m, it can transfer the hash value $h_2(m)$ instead of the whole message to the prover, thereby significantly reducing the communication cost and the computational cost of hashing for the prover in the response phase. The specific construction of Γ-protocols also benefits the online response of the prover, since all the intermediate values irrelevant to the message and used to generate the response can be computed offline. As a result, Γ-based signatures offers an efficient online structure and enjoys the advantage of application flexibility.

Contribution. In this paper, we propose a new structure for the SQIsign family, which is illustrated in Figure 1. The new structure is constructed via Γ-transformation. The main difference between SQIsignHD and our new structure is that the latter one contains an additional isogeny $\varphi_{com} : E_1 \to E_2$, which is derived from the knowledge of the commitment. Besides, the challenge isogeny $\varphi_{chl} : E_A \to E_3$ is hashed from the knowledge of the message. Correspondingly, the response isogeny is from E_2 to E_3.

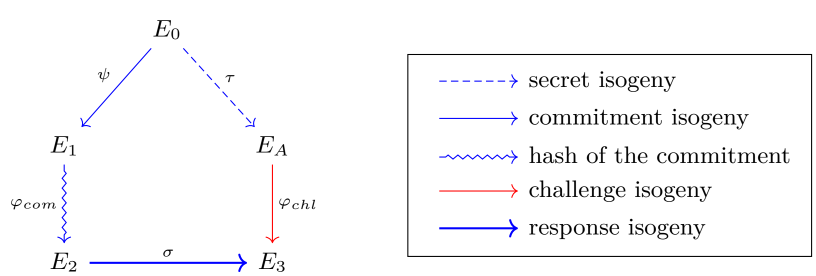


Fig. 1: A sketch of our new structure

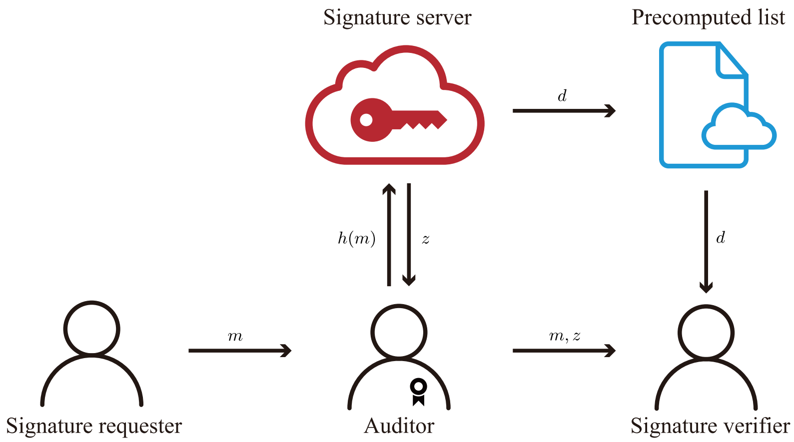
Obviously, our new structure can be easily applied to the SQIsign family. To show the advantages of the new structure compared to the traditional structure, we take SQIsignHD as an instance and introduce ***P**entagon **I**sogeny-based **Sign**ature in **H**igh **D**imension* (referred to as Π-signHD or PIsignHD).

At first glance, the efficiency of Π-signHD appears to be slightly inferior to SQIsignHD due to the additional isogeny involved, which complicates the signing procedure. But in normal cases, SQIsignHD and Π-signHD have the same signature size. Furthermore, Π-signHD has the following additional advantages, which are attractive in applications.

- **Flexible challenge generation**: In SQIsignHD, the challenge isogeny is derived from the knowledge of the public key, the commitment and the message. Benefiting from Γ-transformation, the generation of the challenge isogeny in Π-signHD only requires the public key and the message. This feature tackles the applications as we mentioned above. In Applications 1 and 2, the signature requester can directly transmit the hash value of the message, which reduces transmission and computational requirements for the signer.
- **More compact signature in applications**: The signature of SQIsignHD involves the coefficient of a supersingular curve (or its j-invariant). If the public storage is available, Π-signHD avoids storing it, and the signature size can be reduced from 6.5λ bits to around 3.5λ bits, where λ is the security parameter.
- **Fast online signing computations**: As previously mentioned, the verifier can transfer the kernel of the challenge isogeny directly instead of the whole message, saving the time for the prover to hash the message. Besides, the prover is allowed to precompute intermediate values that are irrelevant to the message. In our implementation, the online signature computations of Π-signHD takes only 4 ms.
- **Storage saving**: To adapt the online/offline technique in SQIsignHD, the prover has to store all the intermediate values that are used to sign the message. Conversely, Π-signHD allows some of the values to be public, or stored on the verifier's size. Therefore, Π-signHD reduces the storage requirements for the prover, which is preferred in applications. We take *Online signature based on hybrid cloud* as an example. Figure 2 illustrates a conceptual scheme for online signature based on Γ-based signatures, suitable for enterprise deployment in a hybrid cloud environment.

  Here are a few points worth noting. First, in Step 2 the auditor only needs to transmit the hash value of the document, instead of the entire document. Second, Step 3 can be done by the signature server in advance, which enhances the efficiency of online signing. Lastly, the verifier retrieves $d = h_1(a)$ from the public cloud in Step 6. This reduces the interaction cost between the auditor and the verifier.

Related Work. Recently, Renan and Kutas proposed a quantum-resistant adaptor signature scheme called SQIAsignHD [32]. This scheme underlies SQIsignHD and utilizes the idea of artificial orientation on SIDH [2]. We believe that some techniques utilized in this work could also be beneficial for SQIAsignHD with further research.



Step 1: The signature requester sends the document m to the auditor.
Step 2: The auditor sends the hash of the document (denoted by $h(m)$) to the signature server. Note that this saves much bandwidth consumption compared to sending m directly.
Step 3: The signature server generates a commitment a and stores the hash of the commitment (denoted by d) in the public cloud.
Step 4: The signature server generates the signature z.
Step 5: The verifier receives the document and the signature.
Step 6: The verifier gets d from the public cloud and verifies the signature.

Fig. 2: Online signature based on Γ-based signatures

Shortly after completing this paper, a number of variants of SQIsignHD are proposed [1,28,17]. Our structure can also be applied to these schemes. More technical details are left as future work.

Organization. The remainder of our paper is organized as follows. Section 2 reviews the preliminaries necessary for this work. In Section 3 we propose a high-level overview of Π-signHD and the underlying identification protocol. The security proofs are provided in Section 4. Section 5 introduces the concrete implementation of Π-signHD, and presents the experimental results. Finally we conclude in Section 6.

2 Preliminaries

In this section we recall the necessary mathematical backgrounds, Σ-protocols, Γ-protocols and SQIsignHD. Especially, we review the current implementation of the signing phase in SQIsignHD in detail.

2.1 Mathematical background

We first provide the necessary mathematical preliminaries, including elliptic curves, isogenies, quaternion algebras, orders and ideals. We refer to [35,37] for more details.

Elliptic Curves. Elliptic curves are nonsingular projective curves with genus 1. For applications, elliptic curves defined in this paper are over a finite field $\mathbb{F}_q$, denoted by $E/\mathbb{F}_q$, where $q = p^n$ with prime $p > 3$ and $n \in \mathbb{N}^*$. An isomorphism class of elliptic curves can be entirely determined by its j-invariant. We use $j(E)$ to denote the j-invariant of E. All the rational points on the elliptic curve E and the point at infinity ∞_E[5] forms an abelian group $E(\mathbb{F}_q)$ under point addition. Let $\ell > 0$, the ℓ-torsion of E is defined as $E[\ell] = \{P \in E(\overline{\mathbb{F}_q}) | [\ell]P = \infty_E\}$, where $[\ell]$ is a multiplication-by-ℓ map. An elliptic curve E is supersingular if $E[p] = \{\infty_E\}$, otherwise E is said to be ordinary.

Isogenies. An isogeny $\varphi : E_1 \to E_2$ is a non-constant surjective morphism that sends ∞_{E_1} to ∞_{E_2}. Denote $\deg(\varphi)$ the degree of φ as a rational map. Two curves E_1 and E_2 are said to be isogenous over $\mathbb{F}_q$ if there exists an isogeny connecting them over $\mathbb{F}_q$. An isogeny φ is called cyclic if its kernel can be generated by one single point P, and separable if the cardinality of the kernel $\ker(\varphi) = \{P \in E_1(\overline{\mathbb{F}_q}) | \varphi(P) = \infty_{E_2}\}$ is equal to $\deg(\varphi)$. If $\deg(\varphi)$ is coprime to the characteristic of the finite field, then φ must be separable. We abbreviate a separable isogeny of degree ℓ as an ℓ-isogeny. Furthermore, for any isogeny $\varphi : E_1 \to E_2$, there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [\deg(\varphi)]$, i.e., the composition of the two isogenies is a multiplication-by-$\deg(\varphi)$ map. In this case, we call $\hat{\varphi}$ the dual isogeny of φ.

Let $\varphi_1 : E_0 \to E_1$ and $\varphi_2 : E_0 \to E_2$ be two separable isogenies with $\gcd(\deg(\varphi_1), \deg(\varphi_2)) = 1$. Then there exist two isogenies $\psi_1 : E_2 \to E_3$ and $\psi_2 : E_1 \to E_3$ such that $\ker(\psi_1) = \varphi_2(\ker(\varphi_1))$ and $\ker(\psi_2) = \varphi_1(\ker(\varphi_2))$, as illustrated in Figure 3. We denote $\psi_1 = [\varphi_2]_*\varphi_1$ (resp. $\psi_2 = [\varphi_1]_*\varphi_2$) as the *pushforward* isogeny of φ_1 (resp. φ_2) through φ_2 (resp. φ_1). Conversely, the isogeny φ_1 (resp. φ_2) is called the *pullback* isogeny of ψ_1 (resp. ψ_2) through φ_2 (resp. φ_1), denoted by $\varphi_1 = [\varphi_2]^*\psi_1$ (resp. $\varphi_2 = [\varphi_1]^*\psi_2$). Note that ψ_1 and ψ_2 are also separable. In addition, there exists an isogeny $\Phi : E_0 \to E_3$ such that $\Phi = \psi_2 \circ \varphi_1 = \psi_1 \circ \varphi_2$.

The supersingular ℓ-isogeny graph is a graph whose vertices represent the supersingular $\overline{\mathbb{F}_p}$ classes and edges represent the equivalent classes of ℓ-isogenies connecting them. The graph is connected, essentially undirected and Ramanujan [31]. Moreover, the graph is $\ell + 1$-regular, meaning that there are exactly $\ell + 1$ equivalent classes of isogenies starting from a given supersingular $\overline{\mathbb{F}_p}$ class.

[5] The point at infinity of an elliptic curve is not necessarily to be indentity, but for simplicity we suppose that it is the identity point.

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

Fig. 3: A commutative isogeny diagram

Endomorphism rings. An endomorphism of E is either an isogeny from E to itself, or the constant morphism $[0]$. The set of all the endomorphisms forms a ring under addition and composition, denoted by $\mathrm{End}(E)$. The endomorphism ring $\mathrm{End}(E)$ is isomorphic to an order in a quaternion algebra if E is supersingular, or an order in a quadratic imaginary field if E is ordinary.
Quaternion algebras, orders and ideals. A quaternion algebra over $\mathbb{Q}$ ramified at p and ∞ has the form $B_{p,\infty} = \mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}k$, where $i^2 = -q$, $j^2 = -p$ and $k = ij = -ji$ with $q \in \mathbb{Z}$. The quaternion algebra has a canonical involution, mapping $\alpha = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k$ to its conjugate $\overline{\alpha} = \alpha_1 - \alpha_2 i - \alpha_3 j - \alpha_4 k$. The reduced trace and the reduced norm of α are defined as $\mathrm{Trd}(\alpha) = 2\alpha_1$ and $\mathrm{Nrd}(\alpha) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$, respectively.

An order in $B_{p,\infty}$ is a full-rank lattice and also a subring. An order is called maximal if it is not contained in other order. A fractional ideal is a $\mathbb{Z}$-lattice of rank 4. Given an ideal I, its left order and right order are defined as

$$\mathcal{O}_L(I) = \{\alpha \in B_{p,\infty} | \alpha I \subset I\}, \mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} | I\alpha \subset I\}.$$

A left (resp. right) $\mathcal{O}$-ideal I is a $\mathbb{Z}$-lattice of rank 4 satisfying that $\mathcal{O} \subset \mathcal{O}_L(I)$ (resp. $\mathcal{O} \subset \mathcal{O}_R I$) and $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$ are maximal. An fractional ideal I is integral if $I \subset \mathcal{O}_L(I)$, which implies that $I \subset \mathcal{O}_R(I)$. Henceforth, we only focus on integral ideals and refer to them as ideals.

An ideal I is said to be invertible, if there exists an ideal I^{-1} such that $II^{-1} = \mathcal{O}_L(I)$ or $I^{-1}I = \mathcal{O}_R(I)$. Denote $\mathrm{Nrd}(I) = \gcd\{\mathrm{Nrd}(\alpha) | \alpha \in I\}$ the reduced norm of I, and $\overline{I} = \{\overline{\alpha} | \alpha \in I\}$ the conjugate of I. If I is invertible, then $I\overline{I} = \mathrm{Nrd}(I)\mathcal{O}_L(I)$ and $\overline{I}I = \mathrm{Nrd}(I)\mathcal{O}_R(I)$. An ideal I of integer reduced norm can be represented by $I = \mathcal{O}_L(I)\alpha + \mathcal{O}_L(I)\mathrm{Nrd}(I)$, where $\alpha \in \mathcal{O}_L(I)$. Two left $\mathcal{O}$-ideals I and J are equivalent if there exists $\beta \in B_{p,\infty}$ such that $I = J\beta$, denoted by $I \sim J$.
Deuring correspondence. The Deuring correspondence provides a link between the world of supersingular elliptic curves and the world of quaternion algebras.

Let E be a supersingular curve, and suppose that the endomorphism ring $\mathrm{End}(E)$ is isomorphic to a maximal order $\mathcal{O}$ of $B_{p,\infty}$. Then an isogeny $\varphi_I : E \to E'$ corresponds to a kernel ideal $I = \{\alpha \in \mathcal{O} | \alpha(P) = \infty_E$ for all $P \in$

$\ker(\varphi_I)\}$, and $\deg(\varphi_I) = \mathrm{Nrd}(I)$. Besides, the left order is isomorphic to $\mathcal{O}$, while the right order is isomorphic to $\mathrm{End}(E')$. In particular, an endomorphism of E corresponds to a principal ideal. Conversely, given a left $\mathcal{O}$-ideal I, the kernel $E[I] = \{P \in E(\overline{\mathbb{F}_p}) | \alpha(P) = \infty_E \text{ for all } \alpha \in I\}$ determines an isogeny φ_I with $\ker(\varphi_I) = E[I]$ and $\deg(\varphi_I) = \mathrm{Nrd}(I)$. The conjugation $\overline{I}$ associates to the dual isogeny $\hat{\varphi}_I$. The multiplication of ideals $I \cdot J$ defines the composition $\varphi_I \circ \varphi_J$, where φ_I and φ_J are two isogenies associated to I and J, respectively. Note that in this case $\mathcal{O}_R(I) \cong \mathcal{O}_L(J)$. In addition, two left $\mathcal{O}$-ideals I and J are equivalent if and only if the isogenies φ_I and φ_J have the same domain and codomain up to isomorphism.

2.2 Σ-Protocol and Fiat–Shamir Paradigm

Assume that P and V are probabilistic polynomial time machines, and the advantage of P over V is that P knows w with $(x, w) \in \mathcal{R}$, where $\mathcal{R}$ is an $\mathcal{NP}$-relation. Now concern the protocols that proceeds as follows:

- P sends a commitment a to V;
- V sends a random string e to P;
- P sends a reply z with respect to e, and V accepts or rejects based on (x, a, e, z).

Definition 1. *Σ-protocol is a three-round public-coin protocol $\langle P, V\rangle$ for an $\mathcal{NP}$-relation $\mathcal{R}$ that proceeds as above. Besides, Σ-protocols should satisfy the following properties:*

- ***Completeness**: V always accepts if P and V follow the protocol.*
- ***Special soundness**: Given two pairs of valid conversations (a, e, z) and (a, e', z') on any input x with $e \neq e'$, one can recover the witness w such that $(x, w) \in \mathcal{R}$ in polynomial time with overwhelming possibility.*
- ***Special honest verifier zero-knowledge (SHVZK)**: There exists a probabilistic polynomial-time simulator $\mathcal{S}$, which takes as input x, and outputs an accepting conversation (a', e', z'), with the same (or computationally indistinguishable) probability distribution as the conversation (a, e, z) of the real protocol.*

Given a Σ-protocol, Fiat–Shamir paradigm [21] can convert it to a signature scheme. The main idea is to set $e = h(a||m)$, where h is a hash function and m is the message. The modification allows the signer to sign the message without interacting with the verifier. The verifier accepts if (a, z) is a valid signature for m [1].

[1] In some specific signature schemes, such as SQIsign [9], the signature can be of form (e, z) since a can be recovered from (e, z).

2.3 Γ-Protocol and Γ-Transformation

Γ-protocol is a special kind of Σ-protocols. Unlike the traditional Σ-protocols, Γ-protocol proceeds as follows:

- P sends a commitment a and a random string d to V;
- V sends a random string e to P;
- P sends a reply z with respect to e, and V accepts or rejects based on (x, a, d, e, z).

Definition 2 ([38]). *Γ-protocol is a three-round public-coin protocol $\langle P, V \rangle$ for an $\mathcal{NP}$-relation $\mathcal{R}$ that proceeds as above. Besides, Γ-protocols should satisfy the following properties:*

- ***Completeness**: V always accepts if P and V follow the protocol.*
- ***Knowledge extraction**: Given two pairs of valid conversations (a, d, e, z) and (a, d', e', z') on any input x with $(d, e) \neq (d', e')$, one can recover the witness w such that $(x, w) \in \mathcal{R}$ in polynomial time with respect to an $\mathcal{NP}$-relation R_e, referred to as e-condition, that $R_e(d, d', e, e', z, z') = 1$. In particular, setting $d = d'$ implies that the protocol has the special soundness property.* [2]
- ***Special honest verifier zero-knowledge (SHVZK)**: There exists a probabilistic polynomial-time simulator $\mathcal{S}$, which takes as input x and outputs an accepting conversation (a', d', e', z'), with the same (or computationally indistinguishable) probability distribution as the conversation (a, d, e, z) of the real protocol.*

Γ-transformation can convey a Γ-protocol into a signature scheme. Different from Fiat-Shamir transform, Γ-transformation adapts two hash functions h_1, h_2 to compute $d = h_1(a)$ and $e = h_2(m)$, respectively. The verifier accepts if $d = h_1(a)$ and (a, d, z) is a valid signature for m [6]. To be precise, Γ-signatures are demonstrated as follows:

- **Key Generation**: The signer generates $x = F(w)$ such that $(x, w) \in \mathcal{R}$ where F is a one-way and polynomial-time computable function. The public key is x and the secret key is w.
- **Signature**: The signer first randomly selects r_P from a set R_P and computes $a = f_a(r_P, x)$, where f_a is a polynomial-time computable function. Then, compute $d = h_1(a)$ where h_1 is a secure hash function. Given a message m, the signer computes $e = h_2(m)$, where h_2 is a secure hash function. From the knowledge of (w, a, d, e) the signer generates z, and finally outputs (a, d, z) as the signature.

[2] The definition here is slightly different from that of [38]. They limits that the knowledge extracts when $\mathcal{R}_e(d, d', e, e') = 1$, where $\mathcal{R}_e$ is an $\mathcal{NP}$-condition. However, Γ-protocol only requires that the e-condition holds with overwhelming possibility.

[6] In some specific signature schemes, such as Γ-signatures for DLP [38], the signature can be compressed by (d, z) since a can be computed according to (d, z).

– **Verification**: Given m, the verifier computes $e = h_2(m)$. The verifier accepts if $d = h_1(a)$ and (a, d, z) is a valid signature for m, according to the polynomial-time computable verification procedure for the underlying Γ-protocol.

2.4 SQIsignHD

SQIsignHD is a compact and post-quantum signature scheme introduced by Dartois, Leroux, Rebort and Wesolowski [11]. It is constructed from an identification protocol via Fiat-Shamir Transform. Currently, there are two versions of SQIsignHD: FastSQIsignHD and RigorousSQIsignHD. In this paper, we focus on constructing a fast online signature scheme based on the FastSQIsignHD version for efficiency. The identification protocols underlying FastSQIsignHD proceeds as follows:

– **Setup**: Select a prime $p = c \cdot \ell^f \cdot \ell'^{f'} - 1$, where $\ell^f \approx \ell'^{f'} \approx 2^\lambda$ with λ the security level. Define a supersingular elliptic curve E_0 defined over $\mathbb{F}_p$ whose endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}$ is known. Let g be an integer big enough but smaller than f.
– **Keygen**: The prover generates a random isogeny walk $\tau : E_0 \to E_A$ of degree $\ell'^{\bullet} \approx p$ and an equivalent isogeny $\tau' : E_0 \to E_A$ of degree $\ell^{\bullet} \approx p$. The public key is the elliptic curve E_A and the secret key is (τ, τ').
– **Commitment**: The prover generates a random (secret) isogeny walk $\psi : E_0 \to E_1$ of degree $\ell'^{\bullet} \approx p$. Afterwards, the prover sends E_1 to the verifier.
– **Challenge**: The verifier generates a random isogeny walk $\varphi : E_A \to E_2$ of degree $\ell'^{f'}$ and sends the description of φ to the prover.
– **Response**: From the knowledge of the secret key, the commitment and the challenge, the prover generates a new isogeny $\sigma : E_1 \to E_2$ of degree q such that q is ℓ^g-good, i.e., $\ell^g - q$ is a prime congruent to 1 modulo 4. Then the prover computes $\sigma(P_1)$ and $\sigma(Q_1)$ where $\langle P_1, Q_1 \rangle$ is the canonical basis of $E_1[\ell^f]$, and sends $(q, \sigma(P_1), \sigma(Q_1))$ to the verifier.
– **Verify**: the verifier generates the canonical basis $\langle P_1, Q_1 \rangle$ of $E_1[\ell^f]$. Then the verifier accepts if $(E_1, E_2, q, (P_1, Q_1), (\sigma(P_1), \sigma(Q_1)))$ correctly represents a q-isogeny σ from E_1 to E_2.

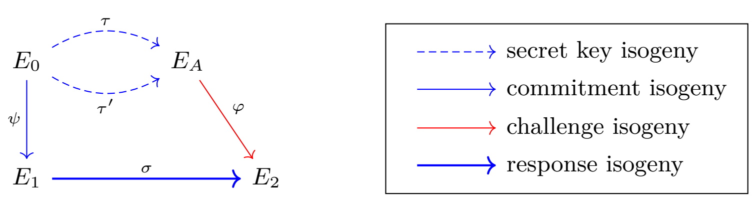


Fig. 4: A sketch of the SQIsignHD identification protocol

Compared with SQIsign, SQIsignHD avoids the complex ideal-to-isogeny translation, and achieves a fast response. The main procedures are illustrated in Algorithm 1.

Algorithm 1 FastRespond [11, Algorithm 2]

Require: The isogenies $\tau, \tau' : E_0 \to E_A$ of degree $\ell'^{\bullet}$ and $\ell^{\bullet}$ respectively, the ideals I_τ and $I_{\tau'}$ associated to τ and τ' respectively, the isogeny $\psi : E_0 \to E_1$ of degree $\ell'^{\bullet}$, the ideal I_ψ associated to ψ, the isogeny $\varphi : E_A \to E_2$ of degree $\ell'^{f'}$.

Ensure: $(\sigma(P_1), \sigma(Q_1), q)$ where (P_1, Q_1) is the canonically determined basis of $E_1[\ell^f]$ and $\sigma : E_1 \to E_2$ is an isogeny of ℓ^g-good degree q prime to ℓ.

1: $I_\varphi \leftarrow$ **IsogenyToIdeal**$(\ker(\varphi), \tau', I_{\tau'})$;
2: $J \leftarrow \overline{I_\psi} \cdot I_\tau \cdot I_\varphi$;
3: $I \leftarrow$ **RandomEquivalentIdeal**$_{\ell^g}(J)$ and compute the reduced norm q of I;
4: If q is not ℓ^g-good or $\gcd(q, \ell') \neq 1$, go back to Line 3;
5: Compute the canonical basis of (P_1, Q_1) of $E_1[\ell^f]$;
6: $(\sigma(P_1), \sigma(Q_1)) \leftarrow$ **EvalTorsion**$_{\ell^f}(I, P_1, Q_1, \psi, \varphi \circ \tau, I_\psi, I_\tau \cdot I_\varphi)$;
7: **return** $(\sigma(P_1), \sigma(Q_1), q)$.

The following are the sub-algorithms applied in Algorithm 1:

– **IsogenyToIdeal**$(\ker(\varphi), \tau', I_{\tau'})$: Given the kernel of an isogeny φ: $E_A \to E_2$, an isogeny τ': $E_0 \to E_A$ of degree coprime to $\deg(\varphi)$ and the corresponding ideal $I_{\tau'} \subset \mathcal{O}$, outputs the ideal I_φ associated to φ;
– **RandomEquivalentIdeal**$_{\ell^g}(J)$: Given an ideal J, ouputs an equivalent ideal I that is uniformly random among ideals of norm $\leq \ell^g$;
– **EvalTorsion**$_{\ell^f}(I, P_1, Q_1, \rho_1, \rho_2, I_{\rho_1}, I_{\rho_2})$: Given an ideal I, a basis $\{P_1, Q_1\}$ of $E_1[\ell^f]$, and two isogenies ρ_1: $E_0 \to E_1$ and ρ_2: $E_0 \to E_2$ and the corresponding ideals I_{ρ_1}, I_{ρ_2}, outputs $\sigma(P_1)$ and $\sigma(Q_1)$, where σ is the isogeny associated to I.

In the response phase, the prover should evaluate the isogeny σ on the basis $\{P_1, Q_1\}$. Since the degree of σ is a non-smooth integer in general, it is difficult to evaluate the isogeny directly with Vélu's formula [36,3]. However, note that the prover has the knowledge of the smooth degree isogenies from E_0 to E_1 and E_2, respectively, i.e., $\psi : E_0 \to E_1$ and $\varphi \circ \tau : E_0 \to E_2$. Furthermore, the endomorphism ring of E_0 is known. Assuming $\mathcal{O}\gamma = I_\psi \cdot I_\sigma \cdot \overline{I_\tau \cdot I_\varphi}$, it is easy to prove that

$$\sigma = \frac{\varphi \circ \tau \circ \gamma \circ \hat{\psi}}{[\deg(\varphi)\deg(\tau)\deg(\psi)]}. \tag{1}$$

Therefore, the prover can evaluate $\sigma(P_1)$ and $\sigma(Q_1)$ efficiently. For more details, we refer to [11, Appendix A.5].

At first glance, the prover still has to evaluate several isogenies to generate the response. Fortunately, the current implementation of SQIsignHD applies a more elegant approach to eliminate almost all the isogeny computations. In the following, we provide a detailed review of the current implementation.

Suppose that $\{P_0, Q_0\}$, $\{P_1, Q_1\}$ and $\{P_A, Q_A\}$ are the canonical bases of $E_0[\ell^f]$, $E_1[\ell^f]$ and $E_A[\ell^f]$, respectively. Then assume

$$\begin{pmatrix} P_A \\ Q_A \end{pmatrix} = M_\tau \begin{pmatrix} \tau(P_0) \\ \tau(Q_0) \end{pmatrix}, \hat{\gamma} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = M_{\hat{\gamma}} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}, \psi \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = M_\psi \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}, \quad (2)$$

where $M_\tau, M_{\hat{\gamma}}, M_\psi \in \mathbb{M}_2(\mathbb{Z}/\ell^f\mathbb{Z})$. Recall from Equation (1) that $\sigma = \varphi \circ \tau \circ \gamma \circ \hat{\psi}/[\deg(\varphi)\deg(\tau)\deg(\psi)]$. Therefore, the prover can compute $\hat{\sigma} \circ \varphi \circ \tau(P_0)$ and $\hat{\sigma} \circ \varphi \circ \tau(Q_0)$ by the following:

$$\begin{aligned} \hat{\sigma} \circ \varphi \circ \tau \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} &= \frac{\psi \circ \hat{\gamma} \circ \hat{\tau} \circ \hat{\varphi} \circ \varphi \circ \tau}{[\deg(\varphi)\deg(\tau)\deg(\psi)]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \\ &= \frac{\psi \circ \hat{\gamma} \circ \hat{\tau} \circ \tau}{[\deg(\tau)\deg(\psi)]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \\ &= \frac{\psi \circ \hat{\gamma}}{[\deg(\psi)]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}. \end{aligned}$$

Since $\hat{\gamma} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = M_{\hat{\gamma}} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}$, one can deduce

$$\hat{\sigma} \circ \varphi \circ \tau \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = \frac{M_{\hat{\gamma}}}{[\deg(\psi)]} \cdot \psi \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}.$$

It follows from $\psi \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = M_\psi \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}$ that

$$\hat{\sigma} \circ \varphi \circ \tau \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = \frac{M_{\hat{\gamma}} \cdot M_\psi}{[\deg(\psi)]} \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}.$$

Note that

$$M_\tau \cdot \begin{pmatrix} \hat{\sigma} \circ \varphi(\tau(P_0)) \\ \hat{\sigma} \circ \varphi(\tau(Q_0)) \end{pmatrix} = \hat{\sigma} \circ \varphi \left(M_\tau \cdot \begin{pmatrix} \tau(P_0) \\ \tau(Q_0) \end{pmatrix} \right) = \hat{\sigma} \circ \varphi \begin{pmatrix} P_A \\ Q_A \end{pmatrix}. \quad (3)$$

Therefore,

$$\hat{\sigma} \circ \varphi \begin{pmatrix} P_A \\ Q_A \end{pmatrix} = \frac{M_\tau \cdot M_{\hat{\gamma}} \cdot M_\psi}{[\deg(\psi)]} \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}.$$

Algorithm 2 summarizes the fast response using the above techniques. The signature is (E_1, q, M), where q is the degree of τ and $M = \frac{M_\tau \cdot M_{\hat{\gamma}} \cdot M_\psi}{[\deg(\psi)]}$. Since φ can be derived from E_1 and the message, the verifier has access to E_2, $\varphi(P_A)$ and $\varphi(Q_A)$. The verifier accepts if $(E_2, E_1, q, (\varphi(P_A), \varphi(Q_A)), (P_1^M, Q_1^M))$ correctly represents an isogeny from E_2 to E_1, where $(P_1^M, Q_1^M)^T = M \cdot (P_1, Q_1)^T$. This is equivalent to prove that σ is an isogeny from E_1 to E_2.

As shown above, the curve coefficient of E_2 is not required for the response generation. Therefore, the prover does not need to construct or evaluate the challenge isogeny φ. Furthermore, the information related to the secret isogeny τ (such as the action matrix M_τ) can be computed during the key generation.

Algorithm 2 FasterRespond

Require: The isogeny $\tau' : E_0 \to E_A$ of degree $\ell'^{\bullet}$, the ideals I_τ and $I_{\tau'}$ associated to τ and τ' respectively, the ideal I_ψ associated to ψ, the isogeny $\varphi : E_A \to E_2$ of degree ℓ^f, and the action matrices M_τ and M_ψ defined in Equation (2).

Ensure: The matrix M such that $(\hat{\sigma} \circ \varphi(P_A), \hat{\sigma} \circ \varphi(Q_A))^T = M \cdot (P_1, Q_1)^T$ and the degree q of the isogeny $\sigma : E_1 \to E_2$.

1: $I_\varphi \leftarrow$ **IsogenyToIdeal**$(\ker(\varphi), \tau', I_{\tau'})$;

2: $J \leftarrow \overline{I_\psi} \cdot I_\tau \cdot I_\varphi$;

3: $I \leftarrow$ **RandomEquivalentIdeal**$_{\ell_1^g}(J)$ and compute the reduced norm q of I;

4: If q is not ℓ_1^g-good or $\gcd(q, \ell_2) \neq 1$, go back to Line 3;

5: Compute $\gamma \in \mathcal{O}$ such that $\mathcal{O}\gamma = I_\psi \cdot I \cdot \overline{I_\tau \cdot I_\varphi}$;

6: Compute the action matrix $M_{\hat{\gamma}}$ as defined in Equation (2);

7: $M \leftarrow \frac{M_\tau \cdot M_{\hat{\gamma}} \cdot M_\psi}{[\deg(\psi)]}$;

8: **return** (M, q).

As a result, the prover only needs to compute the commitment isogeny in the signing phase. All the other computations, such as the generation of the action matrix $M_{\hat{\gamma}}$, are executed over quaternions and linear algebra.

Remark 1. It should be noted that the signature size can be further compressed. For example, the verifier can recover the entire matrix M with only three entries of the action matrix M according to the techniques in [11, Section 6.1]. Furthermore, to verify the validity of the representation the prover can only reveal the actions of the response isogeny on a $\ell^{\lceil g/2 \rceil}$-torsion basis. This halves the storage cost of M. In the meantime, one can set $g \leq 2f$ instead of $g \leq f$ when utilizing **RandomEquivalentIdeal**$_{\ell^g}$ to generate I_σ.[7]

3 *Π*-signHD

In this section we propose the *Π*-signHD identification protocol, and the *Π*-signHD digital signature via *Γ*-transformation.

3.1 Identification protocol

Let λ be a security parameter. The *Π*-signHD identification protocol goes as follows:

- **Setup**: Select a prime $p = c \cdot \ell^f \cdot \ell'^{f'} - 1$, where $\ell^f \approx \ell'^{f'} \approx 2^\lambda$ with λ the security level. Define a supersingular elliptic curve E_0 over $\mathbb{F}_p$ whose endomorphism ring $\mathrm{End}(E) \cong \mathcal{O}$ is known. Let g be an integer big enough but smaller than f.

[7] For efficiency, it is best to set $2f \geq g + 4$. See [11, Section 4.3, Section 4.4] for more details.

- **Keygen**: The prover generates a random isogeny walk $\tau : E_0 \to E_A$ of degree $\ell'^{\bullet} \approx p$ and an equivalent isogeny $\tau' : E_0 \to E_A$ of degree $\ell^{\bullet} \approx p$. The public key is the elliptic curve E_A and the secret key is (τ, τ').
- **Commitment**: The prover generates a random (secret) isogeny walk $\psi : E_0 \to E_1$ of degree $\ell'^{\bullet} \approx p$ and an equivalent isogeny $\psi' : E_0 \to E_1$ of degree $\ell^{\bullet} \approx p$, and then selects a random cyclic isogeny walk $\varphi_{com} : E_1 \to E_2$ of degree $\ell'^{f'}$. Afterwards, the prover sends E_1 and the description of φ_{com} to the verifier.
- **Challenge**: The verifier generates a random isogeny walk $\varphi_{chl} : E_A \to E_3$ of degree $\ell'^{f'}$ and sends the description of φ_{chl} to the prover.
- **Response**: From the knowledge of the secret key, the commitment and the challenge, the prover generates a new isogeny $\sigma : E_2 \to E_3$ of degree q such that q is ℓ^g-good and coprime to ℓ', and computes $\sigma(P_2)$ and $\sigma(Q_2)$ where $\langle P_2, Q_2 \rangle$ is the canonical basis of $E_2[\ell^f]$. Then the prover sends $R = (q, \sigma(P_2), \sigma(Q_2))$ to the verifier.
- **Verify**: the verifier generates the canonical basis $\langle P_2, Q_2 \rangle$ of $E_2[\ell^f]$. Then the verifier accepts if $(E_2, E_3, q, (P_2, Q_2), (\sigma(P_2), \sigma(Q_2)))$ correctly represents a q-isogeny σ from E_2 to E_3.

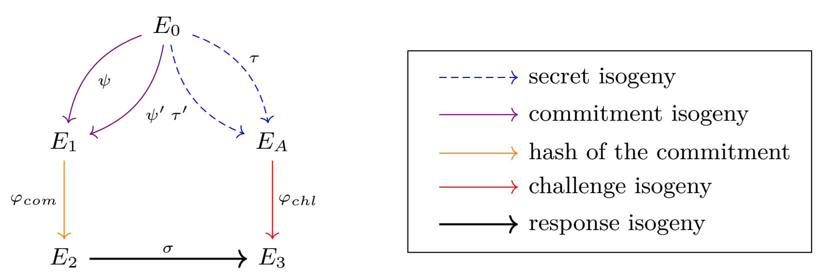


Fig. 5: A sketch of Π-signHD

The completeness property of our Γ-protocol is obvious. The security proofs of the knowledge extraction property and the zero-knowledge property are left in Section 4.

3.2 Digital signature

Via Γ-transformation, Π-signHD is derived by the identification protocol in Section 3.1. The setup and the key generation phases are identical to those of the identification protocol. The signature and the verification proceed as follows:

- **Sign**: $(\mathrm{sk}, m) \to \Sigma$ Pick a random (secret) isogeny $\psi : E_0 \to E_1$ of degree $\ell'^{\bullet} \approx p$ and an equivalent isogeny $\psi' : E_0 \to E_1$ of degree $\ell^{\bullet} \approx p$. Then, construct the cyclic isogeny $\varphi_{com} : E_1 \to E_2$ with respect to the hash of

E_1. From the hash of m, construct the isogeny $\varphi_{chl} : E_A \to E_3$. Finally, generate a new isogeny $\sigma : E_2 \to E_3$ and compute the corresponding pairs $R = (\sigma(P_2), \sigma(Q_2), q)$ with $\{P_2, Q_2\}$ the canonical basis of $E_2[\ell^f]$ and q coprime to ℓ'. The signature is (E_1, R).

– **Verify**: $(\mathrm{pk}, m, \Sigma) \to$ True or False Parse Σ as (E_1, R), where $R = (\sigma(P_2), \sigma(Q_2), q)$. Firstly, compute the isogeny $\varphi_{com} : E_1 \to E_2$ which is hashed from the knowledge of E_1. From the message m, construct the isogeny $\varphi_{chl} : E_A \to E_3$. Generate the determined canonical basis $\langle P_2, Q_2 \rangle = E_2[\ell^f]$, and accept if $(E_2, E_3, q, (P_2, Q_2), (\sigma(P_2), \sigma(Q_2)))$ correctly represents a q-isogeny $\sigma : E_2 \to E_3$.

In the signing and verifying procedures, the isogenies φ_{com} and φ_{chl} are generated by hashing. To achieve this, we first define a secure hash function $\mathcal{H} : \{0,1\}^* \to [1, \mu]$, where $\mu = \ell'^{f'-1}(\ell' + 1)$. Same as SQIsign and SQIsignHD, we use the secure hash function $\mathcal{H}'$ defined in [16, Section 3.1], which is derived from [8]. Taking a supersingular curve E and an integer as inputs, the hash function $\mathcal{H}'$ outputs a cyclic $\ell'^{f'}$-isogeny with domain E. In practice, we set $\varphi_{com} = \mathcal{H}'(E_1, \mathcal{H}(j(E_1)))$ and $\varphi_{chl} = \mathcal{H}'(E_A, \mathcal{H}(m))$.

4 Security Proof

In this section we present the security proofs of Π-signHD. The proof of the completeness property is omitted as it is obvious. In the following we focus on the proofs of the knowledge extraction property and the zero-knowledge property. The knowledge extraction proof is similar to the special soundness proof of the SQIsignHD identification protocol, but a question raised here is that the e-condition must hold with overwhelming probability. We will propose several lemmas to adequately illustrate this issue. The zero-knowledge proof of the Π-signHD identification protocol parallels that of the SQIsignHD identification protocol, particularly we use the same oracle (Definition 3) to construct the simulator.

4.1 Knowledge extraction

Recall the knowledge extraction property of Γ-protocols: Given two pairs of valid conversations (a, d, e, z) and (a, d', e', z') on any input x with $(d, e) \neq (d', e')$, one can recover the witness w such that $(x, w) \in \mathcal{R}$ in polynomial time with respect to an $\mathcal{NP}$-relation $\mathcal{R}_e$, referred to as the e-condition, that $\mathcal{R}_e(d, d', e, e', z, z') = 1$.

In the Π-signHD identification protocol, the commitment is the curve E_1, while φ_{com} is a random isogeny starting from E_1. The challenge corresponds to $\varphi_{chl} : E_A \to E_3$, and the response is of form $R = (q, \sigma(P_2), \sigma(Q_2))$, where q is the degree of the response isogeny $\sigma : E_2 \to E_3$ and $(\sigma(P_2), \sigma(Q_2))$ are the images of the torsion basis $\{P_2, Q_2\}$ of $E_2[\ell^f]$ by σ. The hard problem underlying the knowledge extraction property is known as *Supersingular Endomorphism Problem*:

Problem 1 (Supersingular Endomorphism Problem). Given a prime p and a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, find a non-trivial endomorphism of E that can be efficiently evaluated.

When φ_{com_1} and φ_{com_2} in the two pairs of valid conversations $(E_1, \varphi_{com_1}, \varphi_{chl_1}, R_1)$ and $(E_1, \varphi_{com_2}, \varphi_{chl_2}, R_2)$ are equivalent, the knowledge extraction property is reduced to the special soundness property. In this situation, the proof is almost consistent with the special soundness proofs of the SQIsignHD identification protocol. Similarly, it is easy to prove the knowledge extraction property when the challenges of the valid conversations are equal. When $\varphi_{com_1} \neq \varphi_{com_2}$ and $\varphi_{chl_1} \neq \varphi_{chl_2}$, one can also extract the knowledge under the e-condition that: $\mathcal{R}_e(\varphi_{com_1}, \varphi_{com_2}, \varphi_{chl_1}, \varphi_{chl_2}, \sigma_1, \sigma_2) = 1$ if and only if there does not exist $s \in \mathbb{Z}$ such that $[s] = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$.

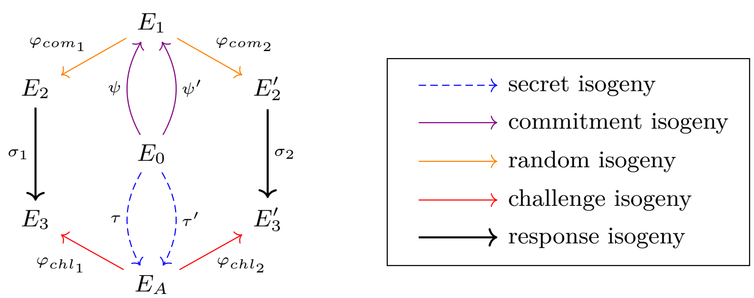


Fig. 6: Knowledge extraction

Proposition 1. *Let $(E_1, \varphi_{com_1}, \varphi_{chl_1}, R_1)$ and $(E_1, \varphi_{com_2}, \varphi_{chl_2}, R_2)$ be two pairs of accepting conversations, where $R_1 = (q_1, \sigma_1(P_2), \sigma_1(Q_2))$ and $R_2 = (q_2, \sigma_2(P_2'), \sigma_2(Q_2'))$ with $\langle P_2, Q_2\rangle = E_2[\ell^f]$ and $\langle P_2', Q_2'\rangle = E_2'[\ell^f]$. If $(\varphi_{com_1}, \varphi_{chl_1}) \neq (\varphi_{com_2}, \varphi_{chl_2})$, then one can compute a non-trivial endomorphism of E_A that can be efficiently evaluated with respect to the e-condition that: $\mathcal{R}_e(\varphi_{com_1}, \varphi_{com_2}, \varphi_{chl_1}, \varphi_{chl_2}, \sigma_1, \sigma_2) = 1$ if and only if there does not exist $s \in \mathbb{Z}$ such that $[s] = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$. If $\varphi_{com_1} = \varphi_{com_2}$ or $\varphi_{chl_1} = \varphi_{chl_2}$, then the e-condition always holds. Especially, the Π-signHD identification protocol has the special soundness property.*

Proof. Since the two conversations are valid, one can obtain the knowledge the response isogenies $\sigma_1 : E_2 \to E_3$ and $\sigma_2 : E_2' \to E_3'$. Note that $\varphi_{com_1} : E_1 \to E_2$, $\varphi_{com_2} : E_1 \to E_2'$, $\varphi_{chl_1} : E_A \to E_3$ and $\varphi_{chl_2} : E_A \to E_3'$ are known. As illustrated in Figure 6, $\alpha = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$ is an endomorphism of E_A that can be efficiently evaluated.

If the e-condition holds, then the endomorphism $\alpha = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$ is non-trivial. Now we prove that the e-condition always holds if $\varphi_{com_1} = \varphi_{com_2}$ or $\varphi_{chl_1} = \varphi_{chl_2}$.

We first prove that the endomorphism α is non-trivial if $\varphi_{com_1} = \varphi_{com_2}$. In this case $\alpha = [\ell'^{2f'}]\hat{\varphi}_{chl_2} \circ \sigma_2 \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$. Suppose for contradiction that $\alpha' = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \hat{\sigma}_1 \circ \varphi_{chl_1} = [s]$ with $s \in \mathbb{Z}$. Therefore, we have $q_1 q_2 \ell'^{2f'} = s^2$. Then

$$[\ell'^{f'} q_2] \circ \hat{\sigma}_1 \circ \varphi_{chl_1} = \hat{\sigma}_2 \circ \varphi_{chl_2} \circ \alpha = [s] \circ \hat{\sigma}_2 \circ \varphi_{chl_2}. \tag{4}$$

Let $s = \ell'^{f'} \cdot s'$ with s' coprime to ℓ'. Then we have $[q_2] \circ \hat{\sigma}_1 \circ \varphi_{chl_1} = [s'] \circ \hat{\sigma}_2 \circ \varphi_{chl_2}$. Since q_1, q_2 and s' are coprime to ℓ', it follows that $\ker(\varphi_{chl_1}) = \ker(\varphi_{chl_2})$. This contradicts the fact that $(\varphi_{com_1}, \varphi_{chl_1}) \neq (\varphi_{com_2}, \varphi_{chl_2})$ and $\varphi_{com_1} = \varphi_{com_2}$. Therefore, the e-condition holds and the Π-signHD identification protocols has the special soundness property.

Assume that $\varphi_{chl_1} = \varphi_{chl_2}$. We would like to prove that α is also non-trivial. Clearly, the endomorphism $\beta = \hat{\varphi}_{com_2} \circ \hat{\sigma}_2 \circ \varphi_{chl_2} \circ \hat{\varphi}_{chl_1} \circ \sigma_1 \circ \varphi_{com_1} = [\ell'^{2f'}]\hat{\varphi}_{com_2} \circ \hat{\sigma}_2 \circ \sigma_1 \circ \varphi_{com_1}$ of E_1 is trivial if and only if α is trivial. Suppose that β is trivial. Similar to the previous proof, one can deduce that $\ker(\varphi_{com_1}) = \ker(\varphi_{com_2})$. This is a contradiction because $(\varphi_{com_1}, \varphi_{chl_1}) \neq (\varphi_{com_2}, \varphi_{chl_2})$ and $\varphi_{chl_1} = \varphi_{chl_2}$. Therefore, when $\varphi_{chl_1} = \varphi_{chl_2}$ the endomorphism β must be non-trivial, i.e., the endomorphism α is non-trivial, which completes the proof. □

It remains to prove that the e-condition holds with overwhelming possibility, i.e.,

$$\Pr\left[\mathcal{R}_e(\varphi_{com_1}, \varphi_{com_2}, \varphi_{chl_1}, \varphi_{chl_2}, \sigma_1, \sigma_2) = 0\right] \leq \mathrm{negl}(\lambda),$$

where $\mathrm{negl}(\cdot)$ is a negligible function. This confirms that even if $\varphi_{com_1} \neq \varphi_{com_2}$ and $\varphi_{chl_1} \neq \varphi_{chl_2}$ (which is the common scenario in practice), the secret key can be extracted with overwhelming possibility once the prover adapts the same commitment. In the following, we present Lemmas 1, 2 and 3 to tackle this problem.

Lemma 1. *Let $\Phi_1 = [\ell'^{t_1}]\Phi'_1$, $\Phi_2 = [\ell'^{t_2}]\Phi'_2$ be two isogenies of degree $(\ell')^{2f'}$, where $\Phi'_1 : E_1 \to E_2$ and $\Phi'_2 : E_3 \to E_4$ are cyclic. Assume that $\sigma : E_2 \to E_3$ and $\sigma' : E_4 \to E_1$ are a q_1-isogeny and a q_2-isogeny with $\gcd(q_1, \ell') = 1$ and $\gcd(q_2, \ell') = 1$, respectively. If $\sigma' \circ \Phi_2 \circ \sigma \circ \Phi_1$ is a trivial endomorphism of E_1, i.e., there exists $s \in \mathbb{Z}$ such that $[s] = \sigma' \circ \Phi_2 \circ \sigma \circ \Phi_1$, then*

- *$t_1 = t_2$;*
- *$[\sigma]_* \widehat{\Phi'_1} = \Phi'_2$, $[\sigma']_* \widehat{\Phi'_2} = \Phi'_1$;*

Proof. From $\Phi_1 = [\ell'^{t_1}]\Phi'_1$, $\Phi_2 = [\ell'^{t_2}]\Phi'_2$, we have

$$[(\ell')^{2f' - t_1 - t_2} s'] = \sigma' \circ \Phi'_2 \circ \sigma \circ \Phi'_1$$

for some $s' = \sqrt{q_1 q_2} \in \mathbb{Z}$ which is coprime to ℓ'.

We first prove $t_1 = t_2$. Without loss of generality, assume by contradiction that $t_1 < t_2$. Since Φ'_1 is cyclic, suppose that $\ker(\Phi'_1) = \langle P \rangle$ where $P \in E_1[(\ell')^{2f' - 2t_1}]$. Then, the endomorphism $[(\ell')^{2f' - t_1 - t_2} s'] = \sigma' \circ \Phi'_2 \circ \sigma \circ \Phi'_1$ sends P to the point at infinity. It implies that $2f' - t_1 - t_2 \geq 2f' - 2t_1$, i.e., $t_1 \geq t_2$, which is a contradiction.

$$\begin{tikzcd}
E_1 \arrow[d, "\Phi_1"'] & E_4 \arrow[l, "\sigma'"'] \\
E_2 \arrow[r, "\sigma"'] & E_3 \arrow[u, "\Phi_2"']
\end{tikzcd}$$

Fig. 7: A sketch of Lemma 1

Now we prove the second claim. Suppose that $Q \in E_1[(\ell')^{2f'-2t_1}]$ such that $\langle P, Q\rangle = E_1[(\ell')^{2f'-2t_1}]$. Then $\ker(\widehat{\Phi_1'}) = \langle \Phi_1'(Q)\rangle$. From $t_1 = t_2$, we have $[(\ell')^{2f'-2t_1}s'] = \sigma' \circ \Phi_2' \circ \sigma \circ \Phi_1'$ and thus $\sigma' \circ \Phi_2' \circ \sigma \circ \Phi_1'(Q) = \infty_{E_1}$, i.e., $\ker(\widehat{\Phi_1'}) \subset \ker(\sigma' \circ \Phi_2' \circ \sigma)$. Since σ and σ' have degrees coprime to ℓ', $\sigma(\ker(\widehat{\Phi_1'})) \subset \ker(\Phi_2')$. It follows from $t_1 = t_2$ that $|\ker(\Phi_2')| = |\sigma(\ker(\widehat{\Phi_1'}))|$. Therefore, $\ker(\Phi_2') = \sigma(\ker(\widehat{\Phi_1'}))$, i.e., $[\sigma]_*\widehat{\Phi_1'} = \Phi_2'$. Analogously, one can imply the other deduction. This ends the proof. $\square$

Remark 2. Lemma 1 shows that if the e-condition does not hold, then $\varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$ is the pushforward isogeny of $\varphi_{com_2} \circ \hat{\varphi}_{com_1}$ through σ_1. Conversely, from $[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$. we cannot deduce the endomorphism $\alpha = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$ is trivial. For example, if $q_1 = \deg(\sigma_1)$ and $q_2 = \deg(\sigma_2)$ are coprime, then in the proof of Lemma 1 the value $s' = \sqrt{q_1q_2} \notin \mathbb{Z}$. In this case the e-condition always holds. Therefore, the possibility that the e-condition does not hold is less than that of $[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$.

Lemma 2. *Let ρ_1, ρ_2, ρ_3, ρ_4 be cyclic $\ell'^{f'}$-isogenies chosen uniformly at random, and $\Phi_1 = \rho_2 \circ \rho_1$ and $\Phi_2 = \rho_4 \circ \rho_3$. If σ is a q-isogeny such that $\gcd(q, \ell') = 1$, then $Pr[[\sigma]_*\Phi_1 = \Phi_2] < (f'+1)(\ell')^{-2f'}$.*

Proof. Suppose that $\Phi_1 = \rho_2 \circ \rho_1 = [\ell^{t_1}]\Phi_1'$ and $\Phi_2 = \rho_4 \circ \rho_3 = [\ell^{t_2}]\Phi_2'$ with Φ_1' and Φ_2' cyclic. To satisfy $[\sigma]_*\Phi_1 = \Phi_2$, we have

$$t_1 = t_2, \sigma(\ker(\Phi_1')) = \ker(\Phi_2').$$

Since ρ_1, ρ_2, ρ_3, ρ_4 are chosen uniformly at random, the possibility that $t_1 = u$ ($t_2 = u$) is

$$\Pr[t_1 = u] = \Pr[t_2 = u] = \begin{cases} \dfrac{\ell'}{\ell'+1}, \text{if } u = 0, \\ \dfrac{\ell'-1}{(\ell'+1)(\ell')^u}, \text{if } 0 < u < f', \\ \dfrac{(\ell')^{1-f'}}{\ell'+1}, \text{if } u = f'. \end{cases}$$

On the other hand, we have

$$\Pr[[\sigma]_*\Phi'_1 = \Phi'_2 | t_1 = t_2 = u] = \begin{cases} \dfrac{(\ell')^{-2f'+2u+1}}{\ell'+1}, \text{if } 0 \le u < f', \\ 1, \text{if } u = f'. \end{cases}$$

Therefore, the possibility that $[\sigma]_*\Phi_1 = \Phi_2$ is

$$\begin{aligned} &\Pr[[\sigma]_*\Phi_1 = \Phi_2] = \Sigma_{u=0}^{f'} \Pr[t_1 = u] \cdot \Pr[t_2 = u] \cdot \Pr\left[[\sigma]_*\Phi'_1 = \Phi'_2 \middle| t_1 = t_2 = u\right] \\ =&\Sigma_{u=0}^{f'} \Pr[t_1 = u]^2 \cdot \Pr\left[[\sigma]_*\Phi'_1 = \Phi'_2 \middle| t_1 = t_2 = u\right] \\ =&\frac{(\ell')^{-2f'+3}}{(\ell'+1)^3} + \Sigma_{u=1}^{f'-1} \frac{(\ell'-1)^2(\ell')^{-2f'+1}}{(\ell'+1)^3} + \frac{(\ell')^{-2f'+2}}{(\ell'+1)^2} \\ =&\frac{(\ell')^3}{(\ell'+1)^3} \cdot (\ell')^{-2f'} + \Sigma_{u=1}^{f'-1} \frac{(\ell'-1)^2\ell'}{(\ell'+1)^3} \cdot (\ell')^{-2f'} + \frac{(\ell')^2}{(\ell'+1)^2} \cdot (\ell')^{-2f'} \\ <&(\ell')^{-2f'} + (f'-1)(\ell')^{-2f'} + (\ell')^{-2f'} \\ =&(f'+1)(\ell')^{-2f'}, \end{aligned}$$

which completes the proof. □

Utilizing Lemmas 1 and 2, we can deduce that the e-condition holds with overwhelming possibility in the case that the prover is honest. Since the isogenies φ_{com_1} and φ_{com_2} are chosen uniformly at random, as stated in Lemma 2 we know that the possibility $\Pr[[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}] < (f'+1)(\ell'^{-2f}) \approx 2^{-2\lambda}$, which is negligible. Therefore, according to Remark 2, the possibility that the e-condition does not hold is also negligible.

Lemma 3. *Let P_1 and P_2 be points of order $\ell'^{f'}$ defined on E_1 and E_2, respectively. Assume that E_1, E_2 are supersingular and $\sigma' : E_1 \to E_2$ is an isogeny whose degree is coprime to ℓ'. If End(E_2) is known, then one can generate $\omega \in$ End(E_2) such that $\omega \circ \sigma'(P_1) = P_2$ in polynomial time.*

Proof. Suppose that $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ is a basis of End(E_2) that can be evaluated at any point of E_2 in polynomial time. Since End$(E_2) \otimes \mathbb{Z}/\ell'^{f'}\mathbb{Z}$ is isomorphic to $\mathbb{M}_2(\mathbb{Z}/\ell'^{f'}\mathbb{Z})$, there exist two endomorphisms in the basis $\{\theta_1, \theta_2, \theta_3, \theta_4\}$, mapping $\sigma'(P_1)$ to points that are linearly independent. For simplicity we assume that $\langle \theta_1(\sigma'(P_1)), \theta_2(\sigma'(P_1)) \rangle = E_2[\ell'^{f'}]$. Then

$$P_2 = [s_1]\theta_1(\sigma'(P_1)) + [s_2]\theta_2(\sigma'(P_1))$$

where $s_1, s_2 \in \mathbb{Z}/\ell'^{f'}\mathbb{Z}$.

Let $\omega = s_1\theta_1 + s_2\theta_2$. Then $\omega \circ \sigma' : E_1 \to E_2$ is the desired isogeny that sends P_1 to P_2. □

Now we argue that the e-condition still holds with overwhelming possibility even if the prover maliciously generates the signature. Firstly, the prover selects a random isogeny φ_{com_1} to the verifier and then the verifier randomly selects an isogeny φ_{chl_1}. To break the e-condition, the best strategy for the malicious prover is to generate σ_1 such that $[\sigma_1]_*\hat{\varphi}_{com_1} = \hat{\varphi}_{chl_1}$, i.e., $\sigma_1(\ker(\hat{\varphi}_{com_1})) = \ker(\hat{\varphi}_{chl_1})$. This procedure can be executed in polynomial time as follows:

1. Generate an isogeny $\sigma' : E_2 \to E_3$;
2. According to Lemma 3, generate an endomorphism ω of E_3 such that $\omega \circ \sigma'(\ker(\hat{\varphi}_{com_1})) = \ker(\hat{\varphi}_{chl_1})$;
3. Set $\sigma_1 = \omega \circ \sigma'$. If $\deg(\sigma_1)$ is not ℓ^g-good with or $\gcd(\deg(\sigma_1), \ell') = 1$, then return to Step 1.

If the e-condition does not hold, then $[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$ from Lemma 1. However, the prover does not have the knowledge of φ_2. Therefore, the possibility that $[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$ holds is $(\ell'+1)^{-1}(\ell')^{-f'+1} \approx 2^{-\lambda}$. Note that if $[\sigma_1]_*(\varphi_{com_2} \circ \hat{\varphi}_{com_1}) = \varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$, the prover can maliciously construct $\sigma_2 = [\varphi_{com_2} \circ \hat{\varphi}_{com_1}]_*\sigma_1$ to break the e-condition. However, it is still hard for the prover to construct an isogeny σ_1 such that $\varphi_{chl_2} \circ \hat{\varphi}_{chl_1}$ is the pushforward isogeny of $\varphi_{com_2} \circ \hat{\varphi}_{com_1}$ through σ_1, as the possibility is negligible.

In summary, we propose the following proposition:

Proposition 2. *In the Π-signHD identification protocol, the e-condition holds with overwhelming possibility. To be precise, assume that $(E_1, \varphi_{com_1}, \varphi_{chl_1}, R_1)$ and $(E_1, \varphi_{com_2}, \varphi_{chl_2}, R_2)$ are two pairs of accepting conversations, where $R_1 = (q_1, \sigma_1(P_2), \sigma_1(Q_2))$ and $R_2 = (q_2, \sigma_2(P_2'), \sigma_2(Q_2'))$ with $\langle P_2, Q_2\rangle = E_2[\ell^f]$ and $\langle P_2', Q_2'\rangle = E_2'[\ell^f]$. If $(\varphi_{com_1}, \varphi_{chl_1}) \neq (\varphi_{com_2}, \varphi_{chl_2})$, then the endomorphism $\alpha = \hat{\varphi}_{chl_2} \circ \sigma_2 \circ \varphi_{com_2} \circ \hat{\varphi}_{com_1} \circ \hat{\sigma}_1 \circ \varphi_{chl_1}$ is non-trivial with overwhelming possibility, no matter if the prover is malicious or not.*

4.2 Zero Knowledge

Same as the security proof for the SQIsignHD identification protocol, we use the following oracle to prove the Π-signHD identification protocol is special honest verifier zero-knowledge.

Definition 3 ([11, Definition 20]). *A random uniform good degree isogeny oracle (RUGDIO) is an oracle taking as input a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and returning an efficient representation $(\sigma(P_1), \sigma(Q_1), q)$ of a random isogeny $\sigma : E \to E'$, where $\{P_1, Q_1\}$ is a canonical basis of $E[\ell^f]$ and q is the degree of σ which is ℓ^g-good and coprime to ℓ'. In addition, the RUGDIO model satisfies that*

- *The distribution of E' is uniform in the supersingular isogeny graph.*
- *The conditional distribution of σ given E is uniform among isogenies from E to E' of ℓ^g-good degree coprime to ℓ'.*

With the help of the RUGDIO model, one can generate an efficient representation of an isogeny starting from a given supersingular elliptic curve E_1, whose degree is ℓ^g-good degree coprime to ℓ'. It has been argued in [11, Section 5.3] that accessing to the oracle does not offer any advantage in reducing the hardness of the *Supersingular Endomorphism Ring Problem* (Problem 2), which can be reduced to *Supersingular Endomorphism Problem* (Problem 1) [18,30]. Same as the SQIsignHD identification protocol, we also have a heuristic assumption on the distribution of the commitment E_1.

Problem 2 (Supersingular Endomorphism Ring Problem). Given a prime p and a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find four endomorphisms of E which can be efficiently evaluated, to form a basis of the endomorphism ring of E.

Proposition 3. *Assume that the commitment E_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph. Then the Π-signHD identification protocol is special honest verifier zero-knowledge in the RUGDIO model. In other words, there exists a simulator $\mathcal{S}$ with access to RUGDIO, satisfying that the distribution of the accepting conversation generated by $\mathcal{S}$ is computationally indistinguishable from the conversation of the Π-signHD identification protocol.*

Proof. We proceed similarly as the zero-knowledge proof of SQIsignHD [11, Theorem 21]. The simulator $\mathcal{S}$ is constructed as follows: Firstly, the simulator $\mathcal{S}$ selects an $\ell'^{f'}$-isogeny $\varphi'_{chl} : E_A \to E'_3$ uniformly at random. After that, the simulator adapts the RUGDIO model to generate an efficient representation R' of $\hat{\sigma'}$ from E'_3 to E'_2, which is also an efficient representation of σ from E'_2 to E'_3. Finally, the simulator $\mathcal{S}$ generates an $\ell'^{f'}$-isogeny $\hat{\varphi}'_{com} : E'_2 \to E'_1$ uniformly at random. The conversation of $\mathcal{S}$ is of form $(E'_1, \varphi'_{com}, R', \varphi'_{chl})$.

Assuming that the conversation of the Π-signHD identification protocol is of form $(E_1, \varphi_{com}, R, \varphi_{chl})$, we aim to prove that the distribution of $(E'_1, \varphi'_{com}, R', \varphi'_{chl})$ is computationally indistinguishable from that of $(E_1, \varphi_{com}, R, \varphi_{chl})$. Applying the RUGDIO model, the curve E'_2 is chosen uniformly at random in the supersingular isogeny graph. Since the isogeny $\hat{\varphi}'_{com} : E'_2 \to E'_1$ is also chosen uniformly at random, it follows that E'_1 is computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph. Therefore, E_1 and E'_1 have the same distribution. Furthermore, the isogenies φ_{com} and φ'_{com} starts from elliptic curves chosen uniformly at random in the supersingular isogeny graph and they are chosen uniformly at random, thus φ_{com} and φ'_{com} have the same distribution. Since $\varphi_{chl} : E_A \to E_3$ and $\varphi'_{chl} : E_A \to E'_3$ are chosen uniformly at random, thus they are indistinguishable.

It remains to prove the efficient representations of σ and σ' are indistinguishable. From the second property of the RUGDIO model, the conditional distribution of $\hat{\sigma'}$ given E'_3 is uniform among isogeny from E'_3 to E'_2, i.e., the conditional distribution of σ' given E'_2 is uniform among isogeny from E'_2 to E'_3. From [11, Section 4.2], σ has the same distribution conditionally to E_2 and E_3. Notably, E_2, E'_2, E_3, E'_3 are computationally indistinguishable from an elliptic curve chosen uniformly at random in the supersingular isogeny graph. This ends the proof. $\square$

5 Implementation and Comparison

In this section, we show how to further reduce the signature size of Π-signHD thanks to the public storage (or the storage of the verifier's size). Besides, we explore how to implement Π-signHD with fast online signing via offline computations, and report the online/offline signature performance results of Π-signHD. Comparisons between SQIsignHD and Π-signHD are also discussed in detail.

5.1 Signature compactness

Recall that the signature of Π-signHD is of the form (E_1, R) where $R = (\sigma(P_2), \sigma(Q_2), q)$: the domain E_1 of the isogeny φ_{com}, the evaluation on the canonical basis $\{P_2, Q_2\}$ of $E_2[\ell^f]$ through σ and the degree of σ. The size is the same as that of SQIsignHD.

Indeed, the signer can also transmit $(E_2, R, \ker(\hat{\varphi}_{com}))$ as the signature: the codomain E_2 of the isogeny φ_{com}, the evaluation on the canonical basis $\{P_2, Q_2\}$ of $E_2[\ell^f]$ through σ, the degree of σ and the kernel of $\hat{\varphi}_{com}$. In this scenario, the signature of Π-signHD involves the additional information $\ker(\hat{\varphi}_{com})$. Therefore, the signature size is larger than that of SQIsignHD. In the following, we show how to compress $(E_2, R, \ker(\hat{\varphi}_{com}))$, making it more compact than the SQIsignHD signature.

Similar to SQIsignHD, one can also compress the torsion basis information utilizing the technique in Section 2.4. Let $\{P_0, Q_0\}$, $\{P_1, Q_1\}$, $\{P_2, Q_2\}$ and $\{P_A, Q_A\}$ be the canonical bases of $E_0[\ell^f]$, $E_1[\ell^f]$, $E_2[\ell^f]$ and $E_A[\ell^f]$, respectively. Assume that

$$\begin{aligned}
\begin{pmatrix} P_A \\ Q_A \end{pmatrix} &= M_\tau \begin{pmatrix} \tau(P_0) \\ \tau(Q_0) \end{pmatrix}, \qquad & \hat{\gamma} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} &= M_{\hat{\gamma}} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}, \\
\psi \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} &= M_\psi \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}, \qquad & \varphi_{com} \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix} &= M_{\varphi_{com}} \begin{pmatrix} P_2 \\ Q_2 \end{pmatrix}.
\end{aligned} \tag{5}$$

where $M_\tau, M_{\hat{\gamma}}, M_\psi, M_{\varphi_{com}} \in \mathbb{M}_2(\mathbb{Z}/\ell^f\mathbb{Z})$. Note that

$$\sigma = \frac{\varphi_{chl} \circ \tau \circ \gamma \circ \hat{\psi} \circ \hat{\varphi}_{com}}{[\deg(\varphi_{chl}) \deg(\tau) \deg(\psi) \deg(\varphi_{com})]}.$$

Then

$$\begin{aligned}
\hat{\sigma} \circ \varphi_{chl} \circ \tau \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} &= \frac{\varphi_{com} \circ \psi \circ \hat{\gamma} \circ \hat{\tau} \circ \hat{\varphi}_{chl} \circ \varphi_{chl} \circ \tau}{[\deg(\varphi_{chl}) \deg(\tau) \deg(\psi) \deg(\varphi_{com})]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \\
&= \frac{\varphi_{com} \circ \psi \circ \hat{\gamma} \circ \hat{\tau} \circ \tau}{[\deg(\tau) \deg(\psi) \deg(\varphi_{com})]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \\
&= \frac{\varphi_{com} \circ \psi \circ \hat{\gamma}}{[\deg(\psi) \deg(\varphi_{com})]} \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix}
\end{aligned}$$

From $\hat{\gamma}\begin{pmatrix}P_0\\Q_0\end{pmatrix} = M_{\hat{\gamma}}\begin{pmatrix}P_0\\Q_0\end{pmatrix}$, we have

$$\hat{\sigma}\circ\varphi_{chl}\circ\tau\begin{pmatrix}P_0\\Q_0\end{pmatrix} = \frac{M_{\hat{\gamma}}}{[\deg(\psi)\deg(\varphi_{com})]}\cdot\varphi_{com}\circ\psi\begin{pmatrix}P_0\\Q_0\end{pmatrix}.$$

Further, it follows from $\psi\begin{pmatrix}P_0\\Q_0\end{pmatrix} = M_{\psi}\begin{pmatrix}P_1\\Q_1\end{pmatrix}$ and $\varphi_{com}\begin{pmatrix}P_1\\Q_1\end{pmatrix} = M_{\varphi_{com}}\begin{pmatrix}P_2\\Q_2\end{pmatrix}$ that

$$\hat{\sigma}\circ\varphi_{chl}\circ\tau\begin{pmatrix}P_0\\Q_0\end{pmatrix} = \frac{M_{\hat{\gamma}}\cdot M_{\psi}}{[\deg(\psi)\deg(\varphi_{com})]}\cdot\varphi_{com}\begin{pmatrix}P_1\\Q_1\end{pmatrix} = \frac{M_{\hat{\gamma}}\cdot M_{\psi}\cdot M_{\varphi_{com}}}{[\deg(\psi)\deg(\varphi_{com})]}\begin{pmatrix}P_2\\Q_2\end{pmatrix}.$$

Same as the deduction in Equation (3):

$$M_{\tau}\cdot\begin{pmatrix}\hat{\sigma}\circ\varphi_{chl}(\tau(P_0))\\\hat{\sigma}\circ\varphi_{chl}(\tau(Q_0))\end{pmatrix} = \hat{\sigma}\circ\varphi_{chl}\left(M_{\tau}\cdot\begin{pmatrix}\tau(P_0)\\\tau(Q_0)\end{pmatrix}\right) = \hat{\sigma}\circ\varphi_{chl}\begin{pmatrix}P_A\\Q_A\end{pmatrix}.$$

Therefore,

$$\hat{\sigma}\circ\varphi_{chl}\begin{pmatrix}P_A\\Q_A\end{pmatrix} = \frac{M_{\tau}\cdot M_{\hat{\gamma}}\cdot M_{\psi}\cdot M_{\varphi_{com}}}{[\deg(\psi)\deg(\varphi_{com})]}\begin{pmatrix}P_2\\Q_2\end{pmatrix}.$$

As a consequence, the signature can be compressed into $(E_2, M, q, \ker(\hat{\varphi}_{com}))$, where

$$M = \frac{M_{\tau}\cdot M_{\hat{\gamma}}\cdot M_{\psi}\cdot M_{\varphi_{com}}}{[\deg(\psi)\deg(\varphi_{com})]} = \frac{M_{\tau}\cdot M_{\hat{\gamma}}\cdot M_{\psi}\cdot M_{\varphi_{com}}}{[\deg(\psi)\ell'^{f'}]}.$$

To store the kernel of $\hat{\varphi}_{com}$, we compress it by finding $k_{\hat{\varphi}_{com}} \in \mathbb{Z}/\ell'^{f'}\mathbb{Z}$ such that $\ker(\hat{\varphi}_{com})$ can be represented by $\langle P_2' + [k_{\hat{\varphi}_{com}}]Q_2'\rangle$ or $\langle Q_2' + [k_{\hat{\varphi}_{com}}]P_2'\rangle$ with $\{P_2', Q_2'\}$ is the canonical basis of $E_2[\ell'^{f'}]$. Note that $\{P_2', Q_2'\}$ can be recovered by the verifier as E_2 is given. Therefore, one can just transfer $(k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}})$ instead of a generator of $\ker(\hat{\varphi}_{com})$, where $label_{\hat{\varphi}_{com}}$ is a bit used to distinguish the two cases mentioned above. This reduces the storage cost of $\ker(\hat{\varphi}_{com})$ to approximately λ bits.

As a Γ-signature, Π-signHD allows the signer to precompute all the intermediate values which are irrelevant to the message. In particular, the signer can precompute plenty of commitments, and store a list of codomains of the hash isogenies $D = \{E_2^{(1)}, E_2^{(2)}, \cdots, E_2^{(n)}\}$ in public, or on the verifier's side. Hence, the signer can transfer the index ind_E in D instead of the codomain of the hash isogeny. Generally, setting $n = 2^{32}$ is enough for practice.

With the help of the list D, the signature of Π-signHD can be compressed into $(ind_E, M, q, (k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}}))$. From Remark 1, the entire action matrix M can be recovered once three entries of it are known, and its size can be further halved by revealing the actions of σ on a $2^{\lceil g/2\rceil}$-torsion basis instead of $\{P_2, Q_2\}$. Therefore, the total storage cost is approximately $32+(3\cdot 0.5\lambda+1)+\lambda+(\lambda+1) = (3.5\lambda+34)$ bits. For comparison, the signature size of SQIsignHD is about 6.5λ bits. For NIST-I security level, $\lambda = 128$, then the signature size of Π-signHD is 519 bits, while the storage cost of SQIsignHD is 870 bits.

5.2 Offline/online signatures

As we mentioned in Section 2.4, the isogeny φ_{chl} can be recovered by the verifier, and the signer can avoid the isogeny computations relevant to φ_{chl}. Besides, the isogenies τ and τ' have been constructed during key generation. Therefore, the main efficiency bottleneck of the response in SQIsignHD is the isogeny computations of the commitment.

In Π-signHD, the signer not only computes the codomain of ψ but an equivalent isogeny ψ' of coprime degree, due to the translation from the isogeny φ_{com} to the associated ideal $I_{\varphi_{com}}$. In addition, the signer has to construct and evaluate the isogeny φ_{com} to obtain the codomain E_2 and the action matrix M_ψ associated to ψ. Fortunately, when implementing online/offline computations, all the above parts can be computed offline and thus they do not affect the efficiency of the online response. Detailed descriptions of the offline/online signatures are presented in Algorithms 3 and 4.

Algorithm 3 Offlinesignature

Require: The initial curve E_0 with known Endomorphism ring.

Ensure: The curve E_2, the action matrix $M_{\varphi_{com}\circ\psi} = M_{\varphi_{com}} \cdot M_\psi$ with $M_{\varphi_{com}}$ and M_ψ defined in Equation (5), the ideal I associated to the isogeny $\varphi_{com} \circ \psi : E_0 \to E_2$, the integer $k_{\hat{\varphi}_{com}}$ and a bit $label_{\hat{\varphi}_{com}}$ used to determine $\ker(\hat{\varphi}_{com})$.

1: Generate a random isogeny walk $\psi : E_0 \to E_1$ of degree $\ell'^{\bullet} \approx p$ and an equivalent isogeny $\psi' : E_0 \to E_1$ of degree $\ell^{\bullet} \approx p$;
2: Compute the ideals I_ψ and $I_{\psi'}$ associated to ψ and ψ', respectively;
3: Compute the canonical bases $\{P_0, Q_0\}$ and $\{P_1, Q_1\}$of $E_0[\ell^f]$ and $E_1[\ell^f]$, respectively;
4: Compute the action matrix M_ψ as defined in Equation (5);
5: $\varphi_{com} \leftarrow \mathcal{H}'(E_1, \mathcal{H}(j(E_1)))$ and compute $\varphi_{com}(P_1)$ and $\varphi_{com}(Q_1)$;
6: Compute $\ker(\hat{\varphi}_{com})$, the kernel of $\hat{\varphi}_{com}$;
7: $I_{\varphi_{com}} \leftarrow$ **IsogenyToIdeal**$(\varphi_{com}, \psi', I_{\psi'})$;
8: Compute the canonical basis $\{P_2', Q_2'\}$ of $E_2[\ell'^{f'}]$;
9: Compute the action matrix $M_{\varphi_{com}}$ as defined in Equation (5);
10: $M_{\varphi_{com}\circ\psi} \leftarrow M_{\varphi_{com}} \cdot M_\psi$, $I \leftarrow I_{\varphi_{com}} \cdot I_\psi$;
11: Find $k_{\hat{\varphi}_{com}} \in \mathbb{Z}/\ell'^{f'}\mathbb{Z}$ such that $\ker(\hat{\varphi}_{com}) = \langle P_2' + [k_{\hat{\varphi}_{com}}]Q_2'\rangle$ or $\ker(\hat{\varphi}_{com}) = \langle [k_{\hat{\varphi}_{com}}]P_2' + Q_2'\rangle$;
12: $label_{\hat{\varphi}_{com}} \leftarrow 1$ if $\ker(\hat{\varphi}_{com}) = \langle P_2' + [k_{\hat{\varphi}_{com}}]Q_2'\rangle$, or $label_{\hat{\varphi}_{com}} \leftarrow 0$ otherwise;
13: $I \leftarrow$ **RandomEquivalentIdeal**$_{\ell^g}(I)$;
14: **return** E_2 and $(M_{\phi\circ\psi}, I, k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}})$.

Remark 3. The signer can compute $\frac{M_{\varphi_{com}\circ\psi}}{\deg(\psi)\ell'^{f'}}$ offline and store it instead of $M_{\varphi_{com}\circ\psi}$ to further improve the online signing performance (Step 7 of Algorithm 4).

The constructions of ψ and ψ' are the efficiency bottlenecks of the offline computations. There are mainly two methods to achieve this: One is to generate ψ uniformly at random, then compute the associated ideal I_ψ and apply

Algorithm 4 Onlinesignature

Require: The isogeny $\tau' : E_0 \to E_A$ of degree $\ell'^{\bullet} \approx p$, the ideals I_τ and $I_{\tau'}$ associated to τ and τ' respectively, the ideal $I_{\varphi_{com}\circ\psi}$ equivalent to $I_{\varphi_{com}} \cdot I_\psi$, the isogeny $\varphi_{chl} : E_A \to E_2$ of degree $\ell'^{f'}$, and the action matrices M_τ and $M_{\varphi_{com}\circ\psi}$ defined in Equation (2).

Ensure: The matrix M such that $(\hat{\sigma} \circ \varphi_{chl}(P_A), \hat{\sigma} \circ \varphi_{chl}(Q_A))^T = M \cdot (P_1, Q_1)^T$ and the degree q of the isogeny $\sigma : E_1 \to E_2$.

1: $I_{\varphi_{chl}} \leftarrow$ **IsogenyToIdeal**$(\varphi_{chl}, \tau', I_{\tau'})$;
2: $J \leftarrow \overline{I_{\varphi_{com}\circ\psi}} \cdot I_\tau \cdot I_{\varphi_{chl}}$;
3: $I \leftarrow$ **RandomEquivalentIdeal**$_{\ell_1^g}(J)$ and compute the reduced norm q of I;
4: If q is not ℓ^g-good or $\gcd(q, \ell') \neq 1$, go back to Line 3;
5: Compute $\gamma \in \mathcal{O}$ such that $\mathcal{O}\gamma = I_\psi \cdot I \cdot \overline{I_\tau \cdot I_{\varphi_{chl}}}$;
6: Compute the action matrix $M_{\hat{\gamma}}$ as defined in Equation (2);
7: $M \leftarrow \frac{M_\tau \cdot M_{\hat{\gamma}} \cdot M_{\varphi_{com}\circ\psi}}{\deg(\psi)\ell'^{f'}}$;
8: **return** (M, q).

the KLPT algorithm [24] to obtain an equivalent ideal, and finally translate it to the associated isogeny ψ' (note that in this case the degree of ψ' is approximately p^3); the other is to generate both of them simultaneously by the elegant techniques utilized in the key generation phase of SQIsignHD [11, Section 3.3]. Our implementation applies the latter one for efficiency reasons. To save the storage cost for the ideal $I_{\varphi_{com}} \circ I_\psi$, the signer can execute the algorithm **RandomEquivalentIdeal**$_{\ell^g}$ to generate an ideal $I \sim I_{\varphi_{com}} \circ I_\psi$ with norm $\mathrm{Nrd}(I) \approx \sqrt{p}$. Note that the codomain E_2 can be public or stored on the verifier's size, while the tuple $(M_{\varphi_{com}\circ\psi}, I, k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}})$ should be secret.

The online signature avoids all the isogeny computations, thus all the operations are over the quaternions and linear algebra. In particular, the efficiency bottleneck of the online signature is the generation of the ideal associated to σ (Lines 3-4 in Algorithm 4). Currently, the approach to obtain the target ideal is somewhat primitive. Finding a more efficient method for the ℓ^g-good equivalent ideal generation is essential to improve the performance of the online signature. We leave it as future work.

We note that the online signing phase of SQIsignHD can also be accelerated via precomputation. Precisely, the signer can precompute the isogeny ψ, the codomain E_1 and the action matrices such as M_ψ in Equation (2). This also avoids the isogeny computations in the online signing phase. However, SQIsignHD has several disadvantages in applications compared with *Π*-signHD when applying the offline/online computations:

– SQIsignHD requires larger storage requirements. To generate a signature with respect to the commitment E_1, the signer has to store I_ψ, M_ψ and E_1. Especially, since the commitment E_1 cannot be public, the signer has to store it before signing. For comparison, *Π*-signHD allows the list $D = \{E_2^{(1)}, E_2^{(2)}, \cdots, E_2^{(s)}\}$ to be public or be stored on the verifier's side. As a consequence, the signer only stores the information $I \sim I_{\varphi_{com}} \cdot I_\psi$, $M_{\varphi_{com}\circ\psi}$,

$(k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}})$ and a label ind_E instead when implementing Π-signHD, reducing the storage cost by approximately 3λ bits for each commitment.
- SQIsignHD has larger signature size. As discussed previously, Π-signHD allows the signer to further compress the signature thanks to the public list D. On the other hand, in SQIsignHD the knowledge of E_1 should be entirely transferred as it is not allowed to be public in advance. Although the signature of Π-signHD also involves the knowledge of the hash isogeny φ_{com}, it is still more compact than that of SQIsignHD due to the large storage requirement of the curve coefficient.
- The challenge isogeny in SQIsignHD is generated from the knowledge of both the commitment E_1 and the message m. Therefore, the online phase in SQIsignHD has to compute the hash of E_1 and m, i.e., $\mathcal{H}(E_1||m)$, and then generate the challenge isogeny $\varphi = \mathcal{H}'(E_A, \mathcal{H}(E_1||m))$. Conversely, in Π-signHD the challenge isogeny $\varphi_{chl} = \mathcal{H}'(E_A, \mathcal{H}(m))$. This is preferred in some specific applications. For example, the hash of the message m can be hashed by a trusted party. In this case, the signer is able to use a low-power device to generate the signature with respect to $\mathcal{H}(m)$, without handling the entire message. When applying SQIsignHD, the signer has to compute $\mathcal{H}(E_1||m)$ or transmit E_1 to the trusted party. The former enlarges the communication cost and the computational cost of online signing, while the latter requires one more round interaction.
- In Π-signHD, the verifier can precompute some intermediate values to fasten the verification. More details are left in the next section.

5.3 Experimental Results

Based on the SQIsignHD code [1], we implement the online/offline signatures of Π-signHD. We benchmark our code on Intel(R) Core(TM) i9-12900K 3.20 GHz with TurboBoost and hyperthreading features disabled.

As mentioned in this last subsection, SQIsignHD also benefits from the online/offline computations. In Table 1 we give an efficiency comparison between the offline/online responses of SQIsignHD and Π-signHD.

As excepted, the online response performance of SQIsignHD and Π-signHD is very fast and close. According to our experimental results, the online response takes only 4 ms. For comparison, the signature of SQIsignHD takes 22.4 ms on average. Therefore, the online response of SQIsignHD/Π-signHD is over 5 times faster than the entire signing procedure of SQIsignHD without offline precomputations.

While the implementation efficiency of online responses of Π-signHD remains unchanged regardless of whether the signature compression is employed, the offline computation is less efficient in the case when using the compression technique. The main reason is that the signer needs to compute the kernel of $\hat{\varphi}_{com}$ and compress it to $(k_{\hat{\varphi}_{com}}, label_{\hat{\varphi}_{com}})$ by computing discrete logarithms during the offline phase of compressed Π-signHD.

[1] `https://github.com/Pierrick-Dartois/SQISignHD-lib`

Table 1: Comparison of the SQIsignHD and Π-signHD signing implementations targeting the NIST-I security level. Benchmarks for our implementation were done on Intel(R) Core(TM) i9-12900K 3.20 GHz with TurboBoost and hyper-threading features disabled. For the performance results (expressed in millions of clock cycles), we execute 1000 times for a 256-bit message and record the average time.

Implementation		SQIsignHD	Π-signHD
Signature size (bits)	Original	870	870
	Compressed	-	519
Clock cycles (cc$\times 10^6$)	Original	70.1	89.8
	Offline (Uncompressed)	57.9	77.8
	Online (Uncompressed)	12.0	11.8
	Offline (Compressed)	-	89.6
	Online (Compressed)	-	11.8

In our implementation, we improve the performance of discrete logarithms in the signing phase by utilizing reduced Tate pairings [25][2]. Indeed, there are some other techniques in the literature which can be utilized to improve the implementation of the offline computations. For instance, one can employ interleaved modular multiplication algorithms [26] to reduce considerable memory loads and stores for multiplications in $\mathbb{F}_{p^2}$. Very recently, faster approaches for pairing computations in isogeny-based protocols are explored by [34,5], which are particularly beneficial for the acceleration of the action matrix computations. We note that in applications the offline computations is connected to the power. Hence, it is acceptable that the offline computations of Π-signHD are not as efficient as that of SQIsignHD.

In summary, the online response performance of both digital signatures is very close, while SQIsignHD has a faster implementation of the offline computations compared to Π-signHD. However, regarding various other advantages as discussed in Section 5.2, Π-signHD appears more promising in practical applications.

Now we analyze the performance of other parts in Π-signHD.

The key generation phase of Π-signHD is identical to that of SQIsignHD, and thus the performance is the same.

When we do not apply the online/offline technique, the verification in Π-signHD needs to construct $\varphi_{com} : E_1 \to E_2$, which is the hash of E_1. Since φ_{com} is a power-smooth isogeny that can be efficiently constructed and evaluated, the overhead is negligible as the isogeny computations in high dimension dominate the computational cost. Therefore, the verification performance of Π-signHD is very close to that of SQIsignHD.

When adapting the online/offline technique, Π-signHD has the potential to achieve a better verification performance compared to SQIsignHD. In addition,

[2] `https://github.com/LinKaizhan/FasterSQISign`

some intermediate values can also be precomputed to fasten the verification, such as the canonical basis, although currently it is not the main bottleneck of the verification. To be precise, the verifier can precompute the canonical basis of any supersingular curve in the list D. Besides, as the challenge isogeny can be generated without any interaction with the signer, the verifier can also compute the canonical basis of the codomain E_3 in advance. We are confident that the isogeny computation in high dimension can be accelerated via precomputation with further research.

6 Conclusion

In this paper we proposed a new structure for the SQIsign family, and proposed Π-signHD based on SQIsignHD. The flexible challenge generation benefits the implementation of Π-signHD in the real-world applications. Furthermore, Π-signHD has a shorter signature size compared with SQIsignHD. In addition, Π-signHD achieves a fast online response via offline computations with cheaper storage requirements.

In our future work, we aim to further enhance the performance of Π-signHD, including reducing the offline storage complexity for the prover, improving the efficiency of offline/online signing and verification, etc. We will also adapt the new structure to other efficient variants of SQIsignHD [10,1,28,17] to make them more competitive in applications. Additionally, it is interesting to develop practical Γ-signatures based on other isogeny-based protocols, such as CSIDH [7] and SIDH-like schemes [22,2].

References

1. Basso, A., Feo, L.D., Dartois, P., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West: The Fast, the Small, and the Safer. Cryptology ePrint Archive, Paper 2024/760 (2024), `https://eprint.iacr.org/2024/760`
2. Basso, A., Fouotsa, T.B.: New SIDH Countermeasures for a More Efficient Key Exchange. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 208–233. Springer Nature Singapore, Singapore (2023)
3. Bernstein, D.J., de Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. In: Galbraith, S. (ed.) ANTS-XIV - 14th Algorithmic Number Theory Symposium. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), vol. 4, pp. 39–55. Mathematical Sciences Publishers, Auckland, New Zealand (2020)
4. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. pp. 227–247. Springer International Publishing, Cham (2019)
5. Cai, S., Lin, K., Zhao, C.A.: Pairing Optimizations for Isogeny-based Cryptosystems. Cryptology ePrint Archive, Paper 2024/575 (2024), `https://eprint.iacr.org/2024/575`

6. Castryck, W., Decru, T.: An Efficient Key Recovery Attack on SIDH. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 423–447. Springer (2023)
7. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24. pp. 395–427. Springer (2018)
8. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic Hash Functions from Expander Graphs. Journal of Cryptology **22**(1), 93–113 (2009)
9. Chavez-Saab, J., Santos, M.C.R., Feo, L.D., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L., Patranabis, S., Petit, C., Henríquez, F.R., Schaeffler, S., Wesolowski, B.: SQIsign (2023), manuscript available at `http://sqisign.org`
10. Corte-Real Santos, M., Eriksen, J.K., Meyer, M., Reijnders, K.: AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 63–93. Springer Nature Switzerland, Cham (2024)
11. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New Dimensions in Cryptography. Cryptology ePrint Archive, Paper 2023/436 (2023), `https://eprint.iacr.org/2023/436`
12. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New Dimensions in Cryptography. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 3–32. Springer Nature Switzerland, Cham (2024)
13. De Feo, L., Galbraith, S.D.: SeaSign: Compact Isogeny Signatures from Class Group Actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 759–789. Springer International Publishing, Cham (2019)
14. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 64–93. Springer International Publishing, Cham (2020)
15. De Feo, L., Leroux, A., Longa, P., Wesolowski, B.: New Algorithms for the Deuring Correspondence: Towards Practical and Secure SQISign Signatures. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 659–690. Springer Nature Switzerland, Cham (2023)
16. De Feo, L., Delpech de Saint Guilhem, C., Fouotsa, T.B., Kutas, P., Leroux, A., Petit, C., Silva, J., Wesolowski, B.: Séta: Supersingular Encryption from Torsion Attacks. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021. pp. 249–278. Springer International Publishing, Cham (2021)
17. Duparc, M., Fouotsa, T.B.: SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. Cryptology ePrint Archive, Paper 2024/773 (2024), `https://eprint.iacr.org/2024/773`
18. Eisenträger, K., Hallgren, S., Lauter, K., Morrison, T., Petit, C.: Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. pp. 329–368. Springer International Publishing, Cham (2018)
19. El Kaafarani, A., Katsumata, S., Pintore, F.: Lossy CSI-FiSh: Efficient Signature Scheme with Tight Reduction to Decisional CSIDH-512. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography – PKC 2020. pp. 157–186. Springer International Publishing, Cham (2020)

20. Even, S., Goldreich, O., Micali, S.: On-Line/Off-Line Digital Signatures. In: Brassard, G. (ed.) Advances in Cryptology — CRYPTO' 89 Proceedings. pp. 263–275. Springer New York, New York, NY (1990)
21. Fiat, A., Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO' 86. pp. 186–194. Springer Berlin Heidelberg, Berlin, Heidelberg (1987)
22. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 282–309. Springer Nature Switzerland, Cham (2023)
23. Galbraith, S.D., Petit, C., Silva, J.: Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. Journal of Cryptology **33**(1), 130–175 (Jan 2020)
24. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS Journal of Computation and Mathematics **17**(A), 418–432 (2014)
25. Lin, K., Wang, W., Xu, Z., Zhao, C.A.: A Faster Software Implementation of SQIsign. IEEE Transactions on Information Theory **70**(9), 6679–6689 (2024)
26. Longa, P.: Efficient Algorithms for Large Prime Characteristic Fields and Their Application to Bilinear Pairings. IACR Transactions on Cryptographic Hardware and Embedded Systems **2023**(3), 445–472 (Jun 2023)
27. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 448–471. Springer (2023)
28. Nakagawa, K., Onuki, H.: SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive, Paper 2024/771 (2024), `https://eprint.iacr.org/2024/771`
29. Onuki, H., Nakagawa, K.: Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign. Cryptology ePrint Archive, Paper 2024/778 (2024), `https://eprint.iacr.org/2024/778`
30. Page, A., Wesolowski, B.: The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 388–417. Springer Nature Switzerland, Cham (2024)
31. Pizer, A.K.: Ramanujan graphs and Hecke operators. Bulletin of the American Mathematical Society **23**(1), 127–137 (1990)
32. Renan, F., Kutas, P.: SQIAsignHD: SQIsignHD Adaptor Signature. Cryptology ePrint Archive, Paper 2024/561 (2024), `https://eprint.iacr.org/2024/561`
33. Robert, D.: Breaking SIDH in polynomial time. In: Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. pp. 472–503. Springer (2023)
34. Robert, D.: Fast pairings via biextensions and cubical arithmetic. Cryptology ePrint Archive, Paper 2024/517 (2024), `https://eprint.iacr.org/2024/517`
35. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd Edition. Graduate Texts in Mathematics. Springer (2009)
36. Vélu, J.: Isogénies entre courbes elliptiques. C. R. Acad. Sci., Paris, Sér. A **273**, 238–241 (1971)
37. Voight, J.: Quaternion algebras. Springer Graduate Texts in Mathematics series. (2021)

38. Yao, A.C.C., Zhao, Y.: Online/Offline Signatures for Low-Power Devices. IEEE Transactions on Information Forensics and Security **8**(2), 283–294 (2013)