A Complete Security Proof of SQIsign

Marius A. Aardal[1(✉)], Andrea Basso[2], Luca De Feo[2], Sikhar Patranabis[3], and Benjamin Wesolowski[4]

[1] Aarhus University, Aarhus, Denmark
maardal@cs.au.dk
[2] IBM Research Europe, Zürich, Switzerland
andrea.basso@ibm.com, crypto25@defeo.lu
[3] IBM Research India, Bangalore, India
sikhar.patranabis@ibm.com
[4] ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France
benjamin.wesolowski@ens-lyon.fr

Abstract. SQIsign is the leading digital signature from isogenies. Despite the many improvements that have appeared in the literature, all its recents variants lack a complete security proof. In this work, we provide the first full security proof of SQIsign, as submitted to the second round of NIST's on-ramp track for digital signatures.

To do so, we introduce a new framework, which we call Fiat–Shamir with hints, that captures all those protocols where the simulator needs additional information to simulate a transcript. Using this framework, we show that SQIsign is EUF-CMA secure in the ROM, assuming the hardness of the One Endomorphism problem *with hints*, or the hardness of the Full Endomorphism Ring problem *with hints* together with a hint indistinguishability assumption; all assumptions, unlike previous ones in the literature, are non-interactive. Along the way, we prove several intermediate results that may be of independent interest.

Keywords: Post-quantum · Isogenies · SQIsign · Security Proof

1 Introduction

SQIsign is a digital signature candidate in NIST's Post-Quantum Cryptography Standardization process [1,11]. Based on the theory of isogenies between supersingular elliptic curves, its security is usually claimed to reduce to the *Supersingular Endomorphism Ring Problem* or, equivalently, to the *Supersingular Isogeny Path Problem* [27]. Despite the claims, the literature only contains incomplete sketches of a security proof, glossing over key details, heuristics, and logical gaps. To complicate matters, since the scheme was first introduced in [14], several variants have appeared [8,13,15,16,21], each calling for different proof techniques.

Y. Tauman Kalai and S. F. Kamara (Eds.): CRYPTO 2025, LNCS 16005, pp. 190–222, 2025.
https://doi.org/10.1007/978-3-032-01887-8_7

In all its incarnations, SQIsign is based on a Σ-protocol which, informally, proves knowledge of the endomorphism ring of a supersingular curve E_{pk}. All variants follow the same pattern:[1]

1. The prover generates a random "commitment curve" E_{com};
2. The verifier challenges with a random isogeny $E_{\mathsf{pk}} \leftrightarrow E_{\mathsf{chl}}$;
3. The prover responds with a random isogeny $E_{\mathsf{com}} \leftrightarrow E_{\mathsf{chl}}$;
4. The verifier checks that the response is a valid isogeny connecting E_{com} to E_{chl} and rejects if that is not the case.

Such a protocol is 2-special-sound: two responses $E_{\mathsf{com}} \leftrightarrow E_{\mathsf{chl}}$ and $E_{\mathsf{com}} \leftrightarrow E'_{\mathsf{chl}}$ to distinct challenges for the same commitment form a cycle $E_{\mathsf{pk}} \leftrightarrow E_{\mathsf{chl}} \leftrightarrow E_{\mathsf{com}} \leftrightarrow E'_{\mathsf{chl}} \leftrightarrow E_{\mathsf{pk}}$ of isogenies and thus an endomorphism of E_{pk}. Although this comes short of a full description of the endomorphism ring, Page and Wesolowski have given a polynomial time reduction from the Endomorphism Ring Problem to the problem of computing a single non-scalar endomorphism [22].

Zero knowledge is much more delicate and crucially depends on the distribution of the response. In the original version of SQIsign and in the first round NIST candidate [11,14,15], the response is a cyclic isogeny of fixed degree 2^x sampled in an algorithmically defined set. It is unknown how to efficiently sample from this distribution without knowledge of the secret key, thus the security proof simulates it with the uniform distribution on all cyclic isogenies of degree 2^x, conjecturing that the associated distinguishing problem is hard. This weak form of zero-knowledge has been the source of several issues, e.g. in [14, Sec. 6] and [10].

In part to bypass the issue above, in part for efficiency, SQIsignHD [13] changed the definition of the response to be any isogeny $E_{\mathsf{com}} \leftrightarrow E_{\mathsf{chl}}$ of any degree up to a certain bound B. The same design was inherited by follow up works [8,16,21] and ultimately by the round-2 candidate [1]. Although sampling from the set of all isogenies up to a certain degree feels more natural and possibly easier to simulate, there is a catch: isogenies of large prime degree can only be efficiently represented using so-called higher-dimensional (HD) representations, which can only be efficiently produced when given a description of the endomorphism rings of the curves, i.e. of the secrets.

Thus, HD variants appear to be even worse than the original SQIsign in terms of zero-knowledge: there is no efficient algorithm to sample from a distribution even remotely similar to the response distribution, without knowledge of the secret. The way SQIsignHD and follow-ups get around this problem is by working with one or more interactive oracles that produce HD-representations of random isogenies of degree $\leq B$. This means that, either explicitly or implicitly, all HD variants have only proved security in an ad-hoc model where every party has access to these oracles producing HD-representations. These proofs do not produce any statement that applies in the more standard Random Oracle Model. Furthermore, these proofs limit themselves to showing special soundness and zero-knowledge of the underlying Σ-protocol: given the ad-hoc nature of

[1] Older variants of SQIsign [11,14] swap the roles of E_{com} and E_{pk} in the challenge and response. Here we focus on the version encountered in the current NIST candidate.

the model, it is unclear whether the standard proof for the Fiat–Shamir transform [23] applies. Thus, all HD variants of SQIsign in the literature fall short of a meaningful security statement.

Contributions. In this work, we give the first full security proof of SQIsign[2] as of the second round of NIST's *on-ramp* track for digital signatures [1]. We innovate on several aspects:

- We introduce a new framework, which we call *Fiat–Shamir with hints*, that captures all those protocols where the simulator needs additional information to simulate a transcript. This framework can be applied to all HD variants of SQIsign, providing the first proof of security in the random oracle model (i.e., without any ad-hoc model) for all those protocols.
- To model the extra information needed by the simulator, previous works introduced interactive oracles to fill the gaps in the simulation. We replace the oracles with non-interactive *hints*, reducing the EUF-CMA security of SQIsign only to non-interactive assumption, whose hardness is easier to analyze. We also study different hints, identifying one type of hints that allows us to reduce the EUF-CMA security of SQIsign to a variant with hints of the endomorphism ring problem and a new indistinguishability problem.
- We carefully account for losses in the reduction, thereby obtaining precise statements on the security of SQIsign's NIST parameters. Based on this, we also make suggestions that have negligible impact on the efficiency of the protocol while benefiting the strength of the security statements.
- Along our security proof, we obtain two smaller results that may be of independent interest: 1. we show that it is possible, in polynomial time, to sample from a distribution statistically close to the distribution of degrees of random isogenies of bounded degree; 2. we show there exists a tight quantum reduction (we only need a factoring oracle) from the endomorphism ring problem to the one endomorphism problem, reducing the runtime loss in the reduction from a factor approximately $2^{94}\log(p)^{13}$ to a factor 24.

1.1 Technical Overview

Fiat–Shamir with hints. We would like to reduce the unforgeability of SQIsign to the $\mathsf{EndRing}_p$problem. However, the protocol does not quite fit into the usual framework for proving security of Fiat–Shamir signatures. In particular, it has two shortcomings:

1. Σ_{SQI} is special-sound, but not with respect to the original relation R_{SQI}.
2. We do not know how to construct a weak Honest-Verifier Zero-Knowledge simulator for Σ_{SQI}. Without knowledge of the endomorphism ring of a curve E, we can only efficiently evaluate random isogenies from E of smooth degree.

[2] The round-2 SQIsign submission slightly diverges from the protocol we analyse: for efficiency reasons, it relies on certain algorithms that may fail with very small probabilities. We discuss this in Sect. 6.

The SQIsign protocol, however, uses isogenies of arbitrary degree in its response: thus, the degree of the simulated response isogenies could not follow the correct distribution.

While the first point only requires a little extra care, the second point is a significant obstacle. Notwithstanding, to the best of current knowledge the hardness of constructing isogenies of arbitrary degree seems independent of that of $\mathsf{EndRing}_p$. If we could give the simulator a little "extra help" to produce these HD representations, then it could simulate the responses without needing to break the scheme.

In Sect. 3, we thus introduce a new framework, which we call *Fiat–Shamir with hints*, for proving EUF-CMA security of Fiat–Shamir signatures where the simulator needs access to some additional data, which allows us to capture protocols like SQIsign and prove their security. We remark that our approach is significantly different from previous literature: all variants of SQIsign that rely on higher-dimensional representations [8,13,16,21] solved the simulation issue by proving security, either explicitly or implicitly, in an ad-hoc model that provides one or more oracles to compute isogenies of arbitrary degree. In contrast, we aim to prove security in the random oracle model, without any additional oracles.

EUF-CMA security of SQIsign. In Sect. 4, we analyze the EUF-CMA security of SQIsign in the Fiat–Shamir with hints framework, using a hint distribution that we call $\mathcal{H}^{\mathsf{sim}}$. We show that Σ_{SQI} has high commitment min-entropy, is hint-assisted wHVZK, and is special-sound with respect to some soundness relation. This gives us our first result, namely that SQIsign is EUF-CMA secure in the ROM, assuming the hardness of the OneEndproblem (i.e. computing one non-trivial endomorphism) with hints.

However, we want to show that SQIsign is EUF-CMA secure as long as the EndRingproblem (i.e. computing *all* endomorphisms) is hard since the EndRingproblem is a much more natural and well-studied problem [17,18,22,27]. In Sect. 5, we obtain a similar result by relying on a variant *with hints* of the EndRingproblem. To do so, however, we cannot rely on the $\mathcal{H}^{\mathsf{sim}}$ hint distribution used so far. The reduction from the EndRingproblem to the OneEndproblem requires translating endomorphisms from one curve to another, and the hint distribution $\mathcal{H}^{\mathsf{sim}}$ enforces a specific distribution that is hard to translate from one curve to another.

We sidestep this issue by introducing a new hint distribution $\mathcal{H}^{\mathsf{unif}}$ that is more suitable for the reduction. In particular, we show that the new hint distribution is *pushable*: given a 2^n-isogeny[3] $\sigma : E \to E'$ and a hint $h \leftarrow \mathcal{H}^{\mathsf{unif}}_E$ for E, we can push it through σ to get a hint for E' distributed according to $\mathcal{H}^{\mathsf{unif}}_{E'}$. We need to introduce a new assumption to switch between distributions (which we argue is hard in Remark 5.1), but the pushability property implies that the new hint distribution $\mathcal{H}^{\mathsf{unif}}$ has several advantages over $\mathcal{H}^{\mathsf{sim}}$:

[3] We use isogenies of degree 2^n because that is the degree of the challenge isogeny in SQIsign, but the distribution is pushable through any smooth-degree isogeny.

- The hint formulation is simpler: the hint does not need to include what becomes the challenge isogeny in a SQIsign transcript since a hint from the public key curve can be pushed to the challenge curve.
- The OneEndproblem with $\mathcal{H}^{\mathsf{unif}}$ hints is equivalent to the EndRingproblem with (the same) hints, which allows us to reduce the hardness of the EndRingproblem with hints to the EUF-CMA security of SQIsign.
- A similar argument shows the EndRingproblem with $\mathcal{H}^{\mathsf{unif}}$ hints is random self-reducible, and thus it admits an average-case to worst-case reduction.
- Lastly, the sampling of hints is conceptually easier, which allows us to provide an argument for why we do not expect these hints to make the EndRing problem easier.

Putting everything together, we obtain a proof of the EUF-CMA security of SQIsign in the ROM, based on the hardness of a variant of the endomorphism ring problem with hints and of the hint indistinguishability problem. When the reduction is classical, the runtime loss in the reduction is about the same as in [22], which is polynomial but considerably large. To obtain a tighter proof of security, we show that quantum reduction (or, equivalently, a classical reduction with access to a factoring oracle) has a runtime loss that is constant and small. This is our main result, which is summarized in Theorem 6.

2 Preliminaries

Notation. We let $\lambda \in \mathbb{N}$ denote the security parameter. All algorithms will (implicitly) take as input the unary encoding of the security parameter 1^λ. We refer to algorithms running in probabilistic polynomial time in the length of their inputs as PPT. We let $\mathsf{poly}(x_1, \ldots, x_n)$ denote an unspecified positive polynomial in $x_1, \ldots, x_n$. Similarly, $\mathsf{negl}(\lambda)$ denotes an unspecified negligible function in λ. When an algorithm $\mathcal{A}$ has black-box query access to an oracle $\mathcal{O}$, we denote this as $\mathcal{A}^{\mathcal{O}}$.

We write ln and log for the natural and the base-2 logarithm respectively. For $x, y \in \{0,1\}^*$, we write $x \parallel y$ for their concatenation and $|x|$ for the length of x.

For a probability distribution D, we write $x \leftarrow D$ for sampling x from D. For a finite set S, we denote the uniform distribution over S by $\mathcal{U}(S)$ and write $x \xleftarrow{\$} S$ for sampling x from $\mathcal{U}(S)$. For two distributions D_0, D_1 over S, the statistical distance between D_0 and D_1 is $\Delta(D_0, D_1) \coloneqq \frac{1}{2} \sum_{s \in S} \left| \Pr\left[D_0 = s\right] - \Pr\left[D_1 = s\right] \right|$. For an algorithm $\mathcal{A}$ outputting a bit b, we define its advantage in distinguishing between D_0 and D_1 as

$$\mathsf{Adv}^{\mathsf{dist}}\left[D_0, D_1\right](\mathcal{A}) \coloneqq \left| \Pr\left[1 \leftarrow \mathcal{A}(x) \;\middle|\; x \leftarrow D_0\right] - \Pr\left[1 \leftarrow \mathcal{A}(x) \;\middle|\; x \leftarrow D_1\right] \right|.$$

Throughout this document, p is a prime congruent to $3 \bmod 4$ of cryptographic size ($p \approx 2^{2\lambda}$). E_A denotes the Montgomery curve $y^2 = x^3 + Ax^2 + x$. We write $\mathsf{Supersingular}_p$ for the set of supersingular Montgomery curves E_A with $A \in \mathbb{F}_{p^2}$ and $j(\mathsf{Supersingular}_p)$ for their j-invariants.

2.1 Computing Isogenies

SQIsign uses three distinct ways to encode and compute with isogenies. It is useful to define a computational abstraction.

Definition 2.1 ([8]). *Let $\mathbb{F}_q$ be a finite field. An isogeny evaluator $\mathscr{E}$ is a pair of polynomial time algorithms:*

- $\mathscr{E}.\mathsf{valid}(D)$*: On input a string $D \in \{0,1\}^*$ it outputs $\perp$ or a triple (E, E', d). In the latter case, E and E' are elliptic curves defined over $\mathbb{F}_q$ and D represents an isogeny $\varphi : E \to E'$ of degree d.*
- $\mathscr{E}.\mathsf{eval}(D, P)$*: On input a string $D \in \{0,1\}^*$ and a point $P \in E(\mathbb{F}_{q^k})$, it outputs the image point $\varphi(P) \in E'(\mathbb{F}_{q^k})$ if $\mathscr{E}.\mathsf{valid}(D) = (E, E', d)$, otherwise the output is undefined.*

In the case that $\mathscr{E}.\mathsf{valid}(D) \neq \perp$ and D is of size polynomial in $\log(q)$ and $\log(d)$, we say that D is an efficient representation of φ (with respect to $\mathscr{E}$).

The first representation used in SQIsign is restricted to isogenies of degree 2^n, represented as 2-*isogeny walks*: the isogeny is stored as a chain $\varphi = \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_n$ of isogenies of degree 2. It is clear this representation is efficient.

The second is the *ideal representation*. If $\mathcal{O} \simeq \mathrm{End}(E)$ is a maximal order of the quaternion algebra ramified at p and ∞, the *Deuring correspondence* establishes a bijection between left ideals of $\mathcal{O}$ and isogenies with domain E. Algorithmically, given a basis of a left ideal of $\mathcal{O}$, there are PPT algorithms to compute the degree and the image of the associated isogeny and to evaluate it on arbitrary points [17,20,27]. This efficient representation intrinsically makes use of the secret key in SQIsign, and is thus only used internally by the prover.

The final representation is the so-called *higher-dimensional (HD) representation*. Following Robert [24], any isogeny between elliptic curves can be "embedded" into an isogeny of higher dimensional abelian varieties using Kani's lemma [19]. SQIsign only uses embeddings into chains of $(2,2)$-isogenies of (2-dimensional) abelian surfaces, which can be efficiently stored and evaluated. Although these yield efficient representations of any isogeny, they are in general difficult to produce in the first place. In SQIsign they are easily computed given knowledge of the secret key, but the difficulty of computing them in general is the key obstacle to proving security which we address in Sect. 3.

Both the ideal and the HD representation support an extended list of additional algorithms operating on them.

Lemma 2.1 (Algorithms on representations). *For each of the operations below there is a PPT algorithm which operates on ideal (resp. HD) representations:*

- ***Dual:*** *On input $\varphi : E_1 \to E_2$, compute $\widehat{\varphi} : E_2 \to E_1$.*
- ***Equality check:*** *On input $\varphi, \psi : E_1 \to E_2$, check whether $\varphi = \psi$.*
- ***Composition:*** *On input $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_3$, compute $\psi \circ \varphi : E_1 \to E_3$.*

- ***Splitting:*** *On input* $\varphi : E_1 \to E_2$ *and coprime* n_1, n_2 *s.t.* $\deg(\varphi) = n_1 n_2$, *find* φ_1, φ_1' *of degree* n_1 *and* φ_2, φ_2' *of degree* n_2 *s.t.* $\varphi = \varphi_2' \circ \varphi_1 = \varphi_1' \circ \varphi_2$.
- ***Division:*** *On input* $\varphi : E_1 \to E_2$, $\varphi_l : E_1 \to E_2'$ *and* $\varphi_r : E_1' \to E_2$, *check if there exist* φ_l', φ_r' *s.t.* $\varphi = \varphi_r' \circ \varphi_l$ *or* $\varphi = \varphi_r \circ \varphi_l'$, *and if so output them.*
- ***Pushforward:*** *On input* $\varphi : E_1 \to E_2$ *and* $\psi : E_1 \to E_3$ *with coprime degrees, compute a pushforward* $\varphi' : E_3 \to E_{23}$ *of* φ *by* ψ, *meaning that* $\ker(\varphi') = \psi(\ker(\varphi))$.
- ***Backtracking:*** *On input* $\varphi : E_2 \to E_3$ *and* $\sigma : E_4 \to E_2$ *with* $\gcd(\deg\varphi, \deg\sigma)$ *smooth, find* ψ, σ', *and* φ' *s.t.* $\sigma = \widehat{\psi} \circ \sigma'$, $\varphi = \varphi' \circ \psi$, *and* $\ker(\psi) = \ker(\varphi) \cap \ker(\widehat{\sigma})$. *We say that* ψ *is the* backtracking component *of* φ *and* σ. *If* φ' *and* σ' *are cyclic, then so is* $\varphi' \circ \sigma'$.

Computational assumptions. We recall two foundational computational problems in isogeny-based cryptography.

Problem 1 (EndRing$_p$). *Given a curve* $E \in \mathsf{Supersingular}_p$, *find four endomorphisms in efficient representation that form a basis of* $\mathrm{End}(E)$ *as a lattice.*

Problem 2 (OneEnd$_p$). *Given a curve* $E \in \mathsf{Supersingular}_p$, *find an endomorphism in* $\mathrm{End}(E) \setminus \mathbb{Z}$ *in efficient representation.*

These problems are believed to computationally hard, even for quantum adversaries. Specifically, we assume that they have worst-case hardness, meaning that no algorithm can solve them in polynomial time in $\log p$ for all curves. This implies that the problems must be hard for uniformly random curves, by well-known worst-case to average-case reductions. Furthermore, a recent line of work [22,27] shows that they are equivalent under polynomial-time reductions.

The stationary distribution S_j is the limit distribution of the random walking process which from a $j(E) \in j(\mathsf{Supersingular}_p)$ selects uniformly at random an ℓ-isogeny $\varphi : E \to E'$ among those that do not backtrack and moves to $j(E')$. [7, Theorem 11] proves the following fact.

Proposition 2.1. *The* stationary distribution S_j *on* $j(\mathsf{Supersingular}_p)$ *is equal to* $S_j(j(E)) = 24/((p-1)|\mathrm{Aut}(E)|)$. *Let* $\ell \neq p$ *be prime. Let* π *be a distribution on* $j(\mathsf{Supersingular}_p)$ *and let* $D_\pi^{\ell^k}$ *be the distribution after* k *steps of a non-backtracking random walk, then* $\Delta(D_\pi^{\ell^k}, S_j) \leq \frac{(k+1)}{4}\sqrt{p/\ell^k}$.

We define the stationary distribution S on $\mathsf{Supersingular}_p$ such that $j^* \leftarrow S_j$ and A is uniformly distributed among those such that $j(E_A) = j^*$.

2.2 The SQIsign Signature Scheme

We recap SQIsign, as submitted to the round-two NIST standardization process for additional post-quantum signatures [1]. It is a Fiat–Shamir signature constructed from a Σ-protocol Σ_{SQI}. We reproduce high-level pseudocode for the protocol; for a more detailed description see [1].

Table 1. The public parameters of SQIsign

Parameter	p	e_{rsp}	e_{chl}	N_{mix}
Description	$p = c \cdot 2^e - 1$ prime, $p < 2^{2\lambda}$, $e \approx 2\lambda$	$\lceil \log_2(\sqrt{p}) \rceil$	$e - e_{\mathsf{rsp}}$	Smallest prime $> 2^{4\lambda}$

Public parameters. For each security level λ, SQIsign defines some public parameters pp, presented in Table 1. We denote the algorithm that deterministically outputs pp by $\mathsf{PublicParam}_{\mathsf{SQI}}(1^\lambda)$. In addition, E_0 denotes the starting curve with j-invariant 1728 and known endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$.

Algorithmic building blocks. We highlight a few recurring algorithmic building blocks in Table 2.

Table 2. Algorithmic building blocks

Algorithm	**Inputs**	**Outputs**
$\mathsf{DeterministicBasis}$	$E \in \mathsf{Supersingular}_p$	A deterministically computed basis (P, Q) for $E[2^e]$.
$\mathsf{IdealToIsogeny}$	Left $\mathcal{O}_0$-ideal I	E_I and (P_I, Q_I), where $\varphi_I : E_0 \to E_I$ corresponds to I, and $P_I, Q_I = \varphi_I(P_0), \varphi_I(Q_0)$, $(P_0, Q_0) = \mathsf{DeterministicBasis}(E_0)$.
$\mathsf{IsogenyEval2\text{-}2}$	$E, E_{12} \in \mathsf{Supersingular}_p$, K_1 and K_2 in $E \times E_{12}$ isotropic[a] of order 2^{f+2}, a list $\mathsf{eval\text{-}pts}$ of points in $E \times E_{12}$.	E_1, E_2 and $[\Phi(P) \mid P \in \mathsf{eval\text{-}pts}]$, where $\Phi : E \times E_{12} \to E_1 \times E_2$ is a deterministically computed $(2^f, 2^f)$-isogeny with $\ker(\Phi) = \langle [4]K_1, [4]K_2 \rangle$.
$\mathsf{MontgomeryRandomize}$	$A \in \mathbb{F}_{p^2}$	$A' \in \mathbb{F}_{p^2}$ uniformly random s.t. $j(E_A) = j(E_{A'})$.
$\mathsf{RandomIdealGivenNorm}$	$N \in \mathbb{N}$ s.t. $p \nmid N$.	Uniformly random primitive left $\mathcal{O}_0$-ideal I of norm N.

[a] Two points of order n are said isotropic if their Weil pairing of order n is trivial.

Relation. The relation of Σ_{SQI} is

$$R_{\mathsf{SQI}} = \left\{ ((\mathsf{pp}, A_{\mathsf{pk}}), I_{\mathsf{sk}}) \;\middle|\; \begin{array}{c} \mathsf{pp} \text{ public parameters,} \\ A_{\mathsf{pk}} \in \mathbb{F}_{p^2},\ E_{\mathsf{pk}} \coloneqq E_{A_{\mathsf{pk}}} \in \mathsf{Supersingular}_p, \\ I_{\mathsf{sk}} \text{ is a left } \mathcal{O}_0\text{-ideal and} \\ \mathcal{O}_R(I_{\mathsf{sk}}) \cong \mathrm{End}(E_{\mathsf{pk}}) \end{array} \right\}.$$

The Montgomery A-invariant A_{pk} will be the public key, and I_{sk} will be the secret key. We can view R_{SQI} as a relation for the $\mathsf{EndRing}_p$ problem, since a basis for $\mathrm{End}(E_{\mathsf{pk}})$ can be efficiently recovered from I_{sk}.

The instance generator $\mathsf{Gen}_{R_{\mathsf{SQI}}}$ is defined in Algorithm 1. The prime N_{mix} is chosen so that $\Delta(j(E_{\mathsf{pk}}), S) \leq 2^{-\lambda}$. In addition, A_{pk} is randomized, to prevent any leakage from the choice of Montgomery coefficient.

Algorithm 1: The instance generator $\mathsf{Gen}_{R_{\mathsf{SQI}}}(1^\lambda)$

1: $\mathsf{pp} \leftarrow \mathsf{PublicParam}_{\mathsf{SQI}}(1^\lambda)$.
2: $I_{\mathsf{sk}} \leftarrow \mathsf{RandomIdealGivenNorm}(N_{\mathsf{mix}})$.
3: $E_A, \_ := \mathsf{IdealToIsogeny}(I_{\mathsf{sk}})$.
4: $A_{\mathsf{pk}} := \mathsf{MontgomeryRandomize}(A)$.
5: $x := (\mathsf{pp}, A_{\mathsf{pk}})$ and $w := I_{\mathsf{sk}}$.
6: **return** (x, w).

The Σ-protocol Σ_{SQI}. The commitment, challenge and response algorithms are presented in Algorithm 2 and the verification algorithm is in Algorithm 3. For an overview of the isogenies involved in the protocol, see Fig. 1.

Remark 2.1. We have modified the description of Σ_{SQI} slightly by adding the lines 24–25 in the response algorithm of Algorithm 2. These steps normalize the points $P_{\mathsf{chl}}, Q_{\mathsf{chl}}$ by making a deterministic choice of sign. This makes the distribution easier to simulate. However, in the optimized implementation of SQIsign, the points are represented by their x-coordinate. Since P_{chl} and $-P_{\mathsf{chl}}$ have the same x-coordinate, this means that the point normalization is not needed there.

Signature scheme. SQIsign is the Fiat–Shamir signature obtained from Σ_{SQI}. We denote it $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$:

- Key generation is identical to $\mathsf{Gen}_{R_{\mathsf{SQI}}}$.
- The signer runs Σ_{SQI} as the prover, using the challenge $\mathsf{chl} \leftarrow \mathsf{RO}(j(E_{\mathsf{com}}) \parallel A_{\mathsf{pk}} \parallel \mathsf{msg})$. The signature is $(\mathsf{chl}, \mathsf{rsp})$.
- The verifier recovers $E_{\mathsf{com}} \simeq F_1$ from the signature[4], checks that it defines a valid isogeny $E_{\mathsf{pk}} \to E_{\mathsf{com}}$ and that $\mathsf{chl} = \mathsf{RO}(j(E_{\mathsf{com}}) \parallel A_{\mathsf{pk}} \parallel \mathsf{msg})$.

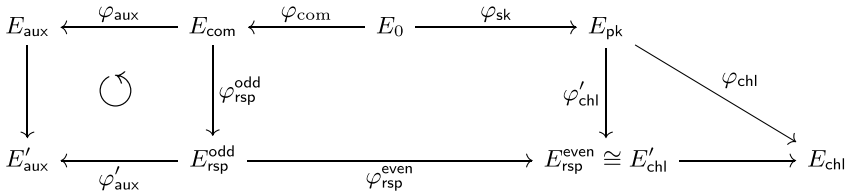

Fig. 1. Diagram of Σ_{SQI}.

[4] SQIsign is *commitment recoverable with perfect uniqueness*, so dropping the commitment from the signature does not affect security [6].

Algorithm 2: The Σ-protocol Σ_{SQI}

Commitment($\mathsf{pp}, A_{\mathsf{pk}}, I_{\mathsf{sk}}$):

$I_{\mathsf{com}} \leftarrow \mathsf{RandomIdealGivenNorm}(N_{\mathsf{mix}})$.
$E_{\mathsf{com}}, (P_{\mathsf{com}}, Q_{\mathsf{com}}) \leftarrow \mathsf{IdealToIsogeny}(I_{\mathsf{com}})$.
$\mathsf{com} \coloneqq j(E_{\mathsf{com}})$; $\mathsf{state} \coloneqq (\mathsf{pp}, A_{\mathsf{pk}}, I_{\mathsf{sk}}, I_{\mathsf{com}}, E_{\mathsf{com}}, P_{\mathsf{com}}, Q_{\mathsf{com}})$.
return com, state.

Challenge:

$\mathsf{chl} \xleftarrow{\$} \{0, \dots, 2^{e_{\mathsf{chl}}} - 1\}$. // Defines the challenge isogeny $\varphi_{\mathsf{chl}} : E_{\mathsf{pk}} \to E_{\mathsf{chl}}$ with $\ker(\varphi_{\mathsf{chl}}) = \langle P_{\mathsf{pk}} + [\mathsf{chl}]Q_{\mathsf{pk}} \rangle$, where $(P_{\mathsf{pk}}, Q_{\mathsf{pk}}) \coloneqq \mathsf{DeterministicBasis}(E_{\mathsf{pk}})$.
return chl.

Response(state, chl):

Compute the left $\mathcal{O}_{\mathsf{pk}}$-ideal I_{chl} corresponding to φ_{chl}, where $\mathcal{O}_{\mathsf{pk}} = \mathcal{O}_R(I_{\mathsf{sk}})$.
Sample a uniformly random ideal J equivalent to $\overline{I_{\mathsf{com}}} \cdot I_{\mathsf{sk}} \cdot I_{\mathsf{chl}}$ of norm $< 2^{e_{\mathsf{rsp}}}$.
Decompose $J = m \cdot I_{\mathsf{rsp}}$ with I_{rsp} a primitive ideal.
// I_{rsp} corresponds to the cyclic response isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.
Write $\mathrm{nrd}(I_{\mathsf{rsp}}) = 2^n d'$ with d' an odd integer.
Let n_{bt} be the largest integer s.t. $I_{\mathsf{chl}} \cdot \overline{I_{\mathsf{rsp}}} \subseteq 2^{n_{\mathsf{bt}}}\mathcal{O}_{\mathsf{pk}}$, and $r' \coloneqq n - n_{\mathsf{bt}}$.
// n_{bt} is the length of the part of $\widehat{\varphi_{\mathsf{rsp}}}$ that backtracks with φ_{chl}.
Factor I_{rsp} as $I_{\mathsf{rsp}}^{(1)} \cdot I_{\mathsf{rsp}}^{(0)} \cdot I'$ s.t. $\mathrm{nrd}(I_{\mathsf{rsp}}^{(1)}) = d'$, $\mathrm{nrd}(I_{\mathsf{rsp}}^{(0)}) = 2^{r'}$, $I_{\mathsf{chl}} \cdot \overline{I'} \subseteq 2^{n_{\mathsf{bt}}}\mathcal{O}_{\mathsf{pk}}$. // $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \xrightarrow{\varphi_{\mathsf{rsp}}^{\mathsf{odd}}} E_{\mathsf{rsp}}^{\mathsf{odd}} \xrightarrow{\varphi_{\mathsf{rsp}}^{\mathsf{even}}} E_{\mathsf{rsp}}^{\mathsf{even}} \xrightarrow{\psi} E_{\mathsf{chl}}$. $\widehat{\psi}$ backtracks φ_{chl}.
$I''_{\mathsf{aux}} \leftarrow \mathsf{RandomIdealGivenNorm}(2^{e_{\mathsf{rsp}}-n} - d')$.
Let I_{aux} be the pushforward of I''_{aux} by I_{com}. // $\varphi_{\mathsf{aux}} : E_{\mathsf{com}} \to E_{\mathsf{aux}}$.
Let I'_{aux} be the pushforward of I_{aux} by $I_{\mathsf{rsp}}^{(1)}$. // $\varphi'_{\mathsf{aux}} : E_{\mathsf{rsp}}^{\mathsf{odd}} \to E'_{\mathsf{aux}}$.
$E'_{\mathsf{aux}}, (K_{\mathsf{aux},1}, K_{\mathsf{aux},2}) \leftarrow \mathsf{IdealToIsogeny}(I_{\mathsf{com}} \cdot I_{\mathsf{rsp}}^{(0)} \cdot I'_{\mathsf{aux}})$.
$K_1 \coloneqq ([2^{e-(e_{\mathsf{rsp}}-n+2)}d']P_{\mathsf{com}},\ [2^{e-(e_{\mathsf{rsp}}-n+2)}]K_{\mathsf{aux},1})$.
$K_2 \coloneqq ([2^{e-(e_{\mathsf{rsp}}-n+2)}d']Q_{\mathsf{com}},\ [2^{e-(e_{\mathsf{rsp}}-n+2)}]K_{\mathsf{aux},2})$.
$\mathsf{eval\text{-}pts} \coloneqq [(P_{\mathsf{com}}, 0), (Q_{\mathsf{com}}, 0)]$.
$E_{\mathsf{rsp}}^{\mathsf{odd}}, E_{\mathsf{aux}}, \mathsf{eval\text{-}pts}' \leftarrow \mathsf{IsogenyEval2\text{-}2}(E_{\mathsf{com}}, E'_{\mathsf{aux}}, K_1, K_2, \mathsf{eval\text{-}pts})$.
Parse $\mathsf{eval\text{-}pts}'$ as $[(R_{\mathsf{chl}}, R_{\mathsf{aux}}), (S_{\mathsf{chl}}, S_{\mathsf{aux}})]$.
$R_{\mathsf{chl}}, S_{\mathsf{chl}} \coloneqq \varphi_{\mathsf{rsp}}^{\mathsf{even}}(R_{\mathsf{chl}}), \varphi_{\mathsf{rsp}}^{\mathsf{even}}(S_{\mathsf{chl}})$.
Compute the non-backtracking part of the challenge isogeny $\varphi'_{\mathsf{chl}} : E_{\mathsf{pk}} \to E'_{\mathsf{chl}}$ with $\ker(\varphi'_{\mathsf{chl}}) = [2^{n_{\mathsf{bt}}}]\ker(\varphi_{\mathsf{chl}})$.
$R_{\mathsf{chl}}, S_{\mathsf{chl}} \coloneqq \iota_{\mathsf{aux}}(R_{\mathsf{chl}}), \iota_{\mathsf{aux}}(R_{\mathsf{chl}})$, for an isomorphism $\iota_{\mathsf{chl}} : E_{\mathsf{rsp}}^{\mathsf{even}} \to E'_{\mathsf{chl}}$.
$A^{\dagger}_{\mathsf{aux}} \leftarrow \mathsf{MontgomeryRandomize}(A_{\mathsf{aux}})$ and $E^{\dagger}_{\mathsf{aux}} \coloneqq E_{A^{\dagger}_{\mathsf{aux}}}$. // $E_{\mathsf{aux}} = E_{A_{\mathsf{aux}}}$.
$R_{\mathsf{aux}}, S_{\mathsf{aux}} \coloneqq \iota_{\mathsf{aux}}(R_{\mathsf{aux}}), \iota_{\mathsf{aux}}(S_{\mathsf{aux}})$, for an isomorphism $\iota_{\mathsf{aux}} : E_{\mathsf{aux}} \to E^{\dagger}_{\mathsf{aux}}$.
$P_{\mathsf{aux}}, Q_{\mathsf{aux}} \coloneqq [2^{e-(e_{\mathsf{rsp}}-n_{\mathsf{bt}}+2)}] \cdot \mathsf{DeterministicBasis}(E^{\dagger}_{\mathsf{aux}})$.
Compute $a, b, c, d \in \mathbb{Z}$ s.t. $P_{\mathsf{aux}} = aR_{\mathsf{aux}} + bS_{\mathsf{aux}}$ and $Q_{\mathsf{aux}} = cR_{\mathsf{aux}} + dS_{\mathsf{aux}}$.
$P_{\mathsf{chl}}, Q_{\mathsf{chl}} \coloneqq (aR_{\mathsf{chl}} + bS_{\mathsf{chl}},\ cR_{\mathsf{chl}} + dS_{\mathsf{chl}})$.
if $-P_{\mathsf{chl}}$ is lexicographically smaller than P_{chl} **then**
    $P_{\mathsf{chl}}, Q_{\mathsf{chl}} \coloneqq -P_{\mathsf{chl}}, -Q_{\mathsf{chl}}$
return $\mathsf{rsp} \coloneqq (n_{\mathsf{bt}}, r', A^{\dagger}_{\mathsf{aux}}, P_{\mathsf{chl}}, Q_{\mathsf{chl}})$.

Algorithm 3: Verification

Input: The statement $(\mathsf{pp}, A_{\mathsf{pk}})$. // A_{pk} determines the public-key curve E_{pk}
Input: The transcript $(, , \mathsf{chl}, \mathsf{rsp})$ with $\mathsf{rsp} = (n_{\mathsf{bt}}, r', A^{\dagger}_{\mathsf{aux}}, P_{\mathsf{chl}}, Q_{\mathsf{chl}})$.
$P_{\mathsf{pk}}, Q_{\mathsf{pk}} \coloneqq \mathsf{DeterministicBasis}(E_{\mathsf{pk}})$.
Compute $E_{\mathsf{pk}}, \varphi'_{\mathsf{chl}} : E_0 \to E'_{\mathsf{chl}}$ with $\ker(\varphi_{\mathsf{chl}}) = \langle [2^{n_{\mathsf{bt}}}](P_{\mathsf{pk}} + [\mathsf{chl}]Q_{\mathsf{pk}})\rangle$.
Check that $E_{\mathsf{pk}}, E^{\dagger}_{\mathsf{aux}} \in \mathsf{Supersingular}_p$, $r' + n_{\mathsf{bt}} \leq e_{\mathsf{rsp}}$,
    and $P_{\mathsf{chl}}, Q_{\mathsf{chl}} \in E'_{\mathsf{chl}}[2^{e_{\mathsf{rsp}} - n_{\mathsf{bt}} + 2}]$; otherwise, **return** 0.
if $r' > 0$ **then**
    if $[2^{e_{\mathsf{rsp}} - n_{\mathsf{bt}} + 1}]P_{\mathsf{chl}} \neq 0$ **then**
        $R \coloneqq [2^{(e_{\mathsf{rsp}} - n_{\mathsf{bt}} + 2) - r'}]P_{\mathsf{chl}}$.
    else if $[2^{e_{\mathsf{rsp}} - n_{\mathsf{bt}} + 1}]Q_{\mathsf{chl}} \neq 0$ **then**
        $R \coloneqq [2^{(e_{\mathsf{rsp}} - n_{\mathsf{bt}} + 2) - r'}]Q_{\mathsf{chl}}$.
    else
        return 0.
    Compute $\varphi : E'_{\mathsf{chl}} \to E_{\mathsf{rsp}}$ with $\ker(\varphi) = \langle R \rangle$.
    $P_{\mathsf{rsp}}, Q_{\mathsf{rsp}} \coloneqq \varphi(P_{\mathsf{chl}}), \varphi(Q_{\mathsf{chl}})$.
$P_{\mathsf{aux}}, Q_{\mathsf{aux}} \coloneqq \mathsf{DeterministicBasis}(E^{\dagger}_{\mathsf{aux}})$.
$K_1 \coloneqq (P_{\mathsf{rsp}}, [2^{e - (e_{\mathsf{rsp}} - n_{\mathsf{bt}} - r' + 2)}]P_{\mathsf{aux}})$.
$K_2 \coloneqq (Q_{\mathsf{rsp}}, [2^{e - (e_{\mathsf{rsp}} - n_{\mathsf{bt}} - r' + 2)}]Q_{\mathsf{aux}})$.
$F_1, F_2, \_ \leftarrow \mathsf{IsogenyEval2\text{-}2}(E_{\mathsf{rsp}}, E^{\dagger}_{\mathsf{aux}}, K_1, K_2, [])$.
if the computation of IsogenyEval2-2 fails **or** $j(F_1) \neq$, **then**
    return 0.
return 1.

3 EUF-CMA-Security from Hard Relations with Hints

3.1 Security Properties

In this section, we define the properties we will need to prove the EUF-CMA-security of $\mathsf{SIG}[\Sigma]$. To help the weak honest-verifier zero-knowledge (wHVZK) simulator, we will give it a hint sampled from a *hint distribution*.

Definition 3.1 (Hint distribution). *Let $R \subseteq \mathcal{X} \times \mathcal{W}$ be a relation. A hint distribution $\mathcal{H}$ for R is a collection of distributions $\mathcal{H} = \{\mathcal{H}_x\}_{x \in \mathcal{X}}$, where $\mathcal{H}_x : \mathsf{HintSet}_x \to [0, 1]$ and the elements (i.e. the hints) of $\mathsf{HintSet}_x$ are efficiently representable in $|x|$. The distribution $\mathcal{H}_x$ need not be efficiently sampleable.*

We define wHVZK with hints as follows.

Definition 3.2 (Hint-assisted wHVZK). *Let $\Sigma = (\mathcal{P}, \mathcal{V})$ be a Σ-protocol for a relation R and let $\mathcal{H}$ be a hint distribution for R. We say that Σ is $\mathcal{H}$-hint-assisted wHVZK if there exists a PPT algorithm, called the simulator $\mathcal{S}$, such that for all $q = \mathsf{poly}(\lambda)$ and all PPT algorithms $\mathcal{A}$*

$$\mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma,\mathcal{H},\mathcal{S}}(\mathcal{A}, q) \coloneqq \mathsf{Adv}^{\mathsf{dist}}\left[\mathsf{Real}_{\Sigma}(1^{\lambda}, q), \mathsf{HintSim}_{\Sigma}(1^{\lambda}, q, \mathcal{S})\right](\mathcal{A}) = \mathsf{negl}(\lambda),$$

where $\mathsf{Real}_{\Sigma}(1^{\lambda}, q)$ and $\mathsf{HintSim}_{\Sigma}(1^{\lambda}, q, \mathcal{S})$ are the distributions in Experiment 1.

For our proof of EUF-CMA-security, we need the relation to remain hard, even if the adversary is given hints.

Experiment 1: Hint-assisted wHVZK

$\underline{\mathsf{Real}_\Sigma(1^\lambda, q)}$:

1: $(x, w) \leftarrow \mathsf{Gen}_R(1^\lambda)$
2: **for** $i = 1$ **to** q **do**
3: $\quad (,_i\, , \mathsf{state}_i) \leftarrow \mathcal{P}_1(x, w)$
4: $\quad \mathsf{chl}_i \xleftarrow{\$} \mathcal{C}$
5: $\quad \mathsf{rsp}_i \leftarrow \mathcal{P}_2(\mathsf{state}_i, \mathsf{chl}_i)$
6: $\quad \pi_i := (,_i\, , \mathsf{chl}_i, \mathsf{rsp}_i)$
7: **return** $(x, \pi_1, \ldots, \pi_q)$

$\underline{\mathsf{HintSim}_\Sigma(1^\lambda, q, \mathcal{S})}$:

1: $(x, w) \leftarrow \mathsf{Gen}_R(1^\lambda)$
2: **for** $i = 1$ **to** q **do**
3: $\quad h_i \leftarrow \mathcal{H}_x$
4: $\quad \pi_i \leftarrow \mathcal{S}(x, h_i)$
5: **return** $(x, \pi_1, \ldots, \pi_q)$

Definition 3.3 (Hard relation with hints). *Let R be a hard relation and let $\mathcal{H}$ be a hint distribution for R. We call the pair $(R, \mathcal{H})$ a relation with hints. We say that it is a hard relation with hints if, in the following game, it holds for all PPT algorithms $\mathcal{A}$ and all $q = \mathsf{poly}(\lambda)$ that*

$$\mathsf{Adv}^{\mathsf{hint\text{-}rel}}_{(R,\mathcal{H})}(\mathcal{A}, q) := \Pr\left[(x, w^*) \in R \;\middle|\; \begin{array}{r}(x, w) \leftarrow \mathsf{Gen}_R(1^\lambda),\\ h_1, \ldots, h_q \leftarrow \mathcal{H}_x,\\ w^* \leftarrow \mathcal{A}(x, h_1, \ldots, h_q)\end{array}\right] = \mathsf{negl}(\lambda).$$

These are all the hint-based security properties we will need. In addition, we will also permit Σ to be special-sound with respect to a different but related relation.

Definition 3.4 (Soundness relation). *Let Σ be a Σ-protocol for the relation R. Consider some relation $\tilde{R} \subseteq \tilde{\mathcal{X}} \times \tilde{\mathcal{W}}$. We say that $\tilde{R}$ is compatible with R if $\mathcal{X} = \tilde{\mathcal{X}}$ and their instance generators sample statements with the same distribution.*

We say that Σ is special-sound with respect to a compatible relation $\tilde{R}$ if given a statement x and two accepting transcripts $(\mathsf{com}, \mathsf{chl}, \mathsf{rsp})$ and $(\mathsf{com}, \mathsf{chl}', \mathsf{rsp}')$ with $\mathsf{chl} \neq \mathsf{chl}'$, we can compute a witness w^* such that $(x, w^*) \in \tilde{R}$ in polynomial time in $|x|$. In this case, we say that $\tilde{R}$ is a soundness relation for Σ.

Observe that if R and $\tilde{R}$ are compatible relations and $\mathcal{H}$ is a hint distribution for R, then it is also a hint distribution for $\tilde{R}$. Additionally, if Σ is special-sound with respect to $\tilde{R}$, then we can always define an instance generator for $\tilde{R}$ so that it is compatible with R. It samples $(x, w) \leftarrow \mathsf{Gen}_R(1^\lambda)$ and then uses the special soundness of Σ to compute a witness w' such that $(x, w') \in \tilde{R}$.

Finally, we recall the notion of the commitment min-entropy of a Σ-protocol.

Definition 3.5 (MinEnt). Σ *has high commitment min-entropy if it holds that*

$$\mathsf{MinEnt}(\Sigma) \coloneqq \max_{(x,w)} \max_{\mathsf{com}} \Pr\left[\mathsf{com} = \mathsf{com}' \;\middle|\; (\mathsf{com}', \mathsf{state}) \leftarrow \mathcal{P}_1(x, w)\right] = \mathsf{negl}(\lambda),$$

where the first max ranges over the pairs that might be output by $\mathsf{Gen}_R(1^\lambda)$.

3.2 Reducing the Hard Relations with Hints to EUF-CMA

Let $(R, \mathcal{H})$ be a relation with hints and let Σ be a Σ-protocol for R. In this section, we identify the following conditions for $\mathsf{SIG}[\Sigma]$ to be EUF-CMA-secure:

1. Σ has high commitment min-entropy.
2. Σ is $\mathcal{H}$-hint-assisted wHVZK.
3. Σ is special-sound with respect to a soundness relation $\tilde{R}$.
4. Σ has a challenge space $\mathcal{C}$ of exponential size in λ.
5. $(\tilde{R}, \mathcal{H})$ is a hard relation with hints.

We prove this by a chain of reductions. The first step is standard: given that Σ has high commitment min-entropy, we reduce the security against impersonation attacks (IMP-PA) of Σ to the EUF-CMA security of $\mathsf{SIG}[\Sigma]$ (cf. [3] for more details).

The next step will be to use the hint-assisted wHVZK. We will use it to simulate the transcript oracle OTrans in the IMP-PA game. For this purpose, we consider the intermediate game hint-IMP-PA in Definition 3.6. In this game, the adversary no longer has access to the transcript oracle OTrans. Instead, it is given hints from which it can simulate its own transcripts. Hence, we can view this game as a noninteractive variant of the IMP-PA game.

Definition 3.6 (hint-IMP-PA). *Let* $(R, \mathcal{H})$ *be a relation with hints and let* Σ *be a* Σ*-protocol for* R*. We say that* Σ *is secure under* $\mathcal{H}$*-hint-assisted passive impersonation attacks (*$\mathcal{H}$-hint-IMP-PA*) if for all* $q = \mathsf{poly}(\lambda)$ *and all PPT two-stage algorithms* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *it holds that*

$$\mathsf{Adv}^{\mathsf{hint\text{-}IMP\text{-}PA}}_{\Sigma,\mathcal{H}}(\mathcal{A}, q) \coloneqq \Pr\left[\mathcal{H}\text{-}\mathsf{hint\text{-}IMP\text{-}PA}_\Sigma(\mathcal{A}, q) = 1\right] = \mathsf{negl}(\lambda),$$

where $\mathcal{H}$-hint-IMP-PA$_\Sigma$ *is the game presented in Game 1.*

Lemma 3.1. *Let* $(R, \mathcal{H})$ *be a relation with hints and let* Σ *be a* Σ*-protocol for the relation* R*. Additionally, let* $\mathcal{S}$ *be a* $\mathcal{H}$*-assisted simulator for* Σ*.*

For any two-stage PPT algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *against the* IMP-PA *of* Σ*, there exists a two-stage PPT algorithm* $\mathcal{B}$ *and a PPT algorithm* $\mathcal{D}$ *such that*

$$\mathsf{Adv}^{\mathsf{IMP\text{-}PA}}_{\Sigma}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{hint\text{-}IMP\text{-}PA}}_{\Sigma,\mathcal{H}}(\mathcal{B}, q) + \mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma,\mathcal{H},\mathcal{S}}(\mathcal{D}, q),$$

where q *is an upper-bound on the number of queries that* $\mathcal{A}_1$ *makes to* OTrans.

Game 1: $\mathcal{H}$-hint-IMP-PA$_\Sigma(\mathcal{A}_1, \mathcal{A}_2, q)$

1: $(x, w) \leftarrow \mathsf{Gen}_R(1^\lambda)$
2: $h_1, \ldots, h_q \leftarrow \mathcal{H}_x$
3: $(, , \mathsf{state}) \leftarrow \mathcal{A}_1(x, h_1, \ldots, h_q)$
4: $\mathsf{chl} \xleftarrow{\$} \mathcal{C}$
5: $\mathsf{rsp} \leftarrow \mathcal{A}_2(\mathsf{state}, \mathsf{chl})$
6: $b \coloneqq \mathsf{Ver}_\Sigma(x, , , \mathsf{chl}, \mathsf{rsp}) = 1$
7: **return** b

Proof. We will use $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ and $\mathcal{S}$ to construct an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{A}_2)$ for the hint-IMP-PA game. $\mathcal{B}$ has the same second stage algorithm as $\mathcal{A}$.

$\mathcal{B}_1$ takes as input a statement x sampled from $\mathsf{Gen}_R(1^\lambda)$ and q hints $h_1, \ldots, h_q \leftarrow \mathcal{H}_x$. It then runs $\mathcal{A}_1$ on input x. Whenever $\mathcal{A}_1$ makes a query to the transcript oracle OTrans, $\mathcal{B}_1$ responds using the simulator $\mathcal{S}$. For the ith query, $\mathcal{B}_1$ runs $(\mathsf{com}_i, \mathsf{chl}_i, \mathsf{rsp}_i) \leftarrow \mathcal{S}(x, h_i)$ and responds with $(\mathsf{com}_i, \mathsf{chl}_i, \mathsf{rsp}_i)$. When $\mathcal{A}_1$ outputs $(\mathsf{com}^*, \mathsf{state}^*)$, $\mathcal{B}_1$ outputs the same and terminates.

We use the hint-assisted wHVZK of Σ to relate the advantage of $\mathcal{B}$ in the hint-IMP-PA game to the advantage of $\mathcal{A}$ in the IMP-PA game. If there is a difference in success probability, we can construct a distinguisher $\mathcal{D}$. On input $(x, \boldsymbol{\pi})$ with $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_q)$, $\mathcal{D}$ runs the IMP-PA game for $\mathcal{A}$ and answers the ith query to OTrans with π_i. Finally, $\mathcal{D}$ outputs the same bit as the game. We have

$$\mathsf{Adv}^{\mathsf{IMP\text{-}PA}}_{\Sigma}(\mathcal{A}) = \Pr\left[1 \leftarrow \mathcal{D}(x, \boldsymbol{\pi}) \;\middle|\; (x, \boldsymbol{\pi}) \leftarrow \mathsf{Real}_\Sigma(1^\lambda, q)\right] \text{ and}$$
$$\mathsf{Adv}^{\mathsf{hint\text{-}IMP\text{-}PA}}_{\Sigma,\mathcal{H}}(\mathcal{B}, q) = \Pr\left[1 \leftarrow \mathcal{D}(x, \boldsymbol{\pi}) \;\middle|\; (x, \boldsymbol{\pi}) \leftarrow \mathsf{HintSim}_\Sigma(1^\lambda, q)\right].$$

Hence,

$$\mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma,\mathcal{H},\mathcal{S}}(\mathcal{A}, q) = |\mathsf{Adv}^{\mathsf{IMP\text{-}PA}}_{\Sigma}(\mathcal{A}) - \mathsf{Adv}^{\mathsf{hint\text{-}IMP\text{-}PA}}_{\Sigma,\mathcal{H}}(\mathcal{B}, q)|. \qquad \square$$

Finally, we use the special soundness of Σ to reduce the hardness of $(\tilde{R}, \mathcal{H})$ to the hint-IMP-PA-security of Σ.

Lemma 3.2. *Let $(R, \mathcal{H})$ be a relation with hints and let Σ be a Σ-protocol for the relation R with challenge space $\mathcal{C}$. Additionally, assume Σ is special-sound with respect to the soundness relation $\tilde{R}$.*

For any two-stage PPT algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ playing the hint-IMP-PA *game for Σ with q hints from $\mathcal{H}$, there exists an expected polynomial time algorithm $\mathcal{B}$ playing the game for $(\tilde{R}, \mathcal{H})$ such that*

$$\mathsf{Adv}^{\mathsf{hint\text{-}IMP\text{-}PA}}_{\Sigma,\mathcal{H}}(\mathcal{A}, q) \leq \mathsf{Adv}^{\mathsf{hint\text{-}rel}}_{(\tilde{R},\mathcal{H})}(\mathcal{B}, q) + \frac{1}{|\mathcal{C}|}.$$

Proof. By [4], Σ is knowledge-sound with respect to $\tilde{R}$, with knowledge error $1/|\mathcal{C}|$. Let $\mathcal{E}$ be the knowledge extractor.

We begin by describing the adversary $\mathcal{B}$ against the hard relation with hints $(\tilde{R}, \mathcal{H})$. It gets as input a statement x generated by $\mathsf{Gen}_{\tilde{R}}(1^\lambda)$ and hints $h_1, \ldots, h_q \leftarrow \mathcal{H}$. This is exactly the same input distribution that $\mathcal{A}$ gets in its hint-IMP-PA game. $\mathcal{B}$ fixes the inputs of $\mathcal{A}$ to be $x, h_1, \ldots, h_q$, then runs $\mathcal{E}$ on $\mathcal{A}$.

Let us analyze the success probability of $\mathcal{B}$. Let X and $\boldsymbol{H}$ be random variables distributed as the statement and the q hints in the inputs to $\mathcal{A}$ and $\mathcal{B}$. Let $A(X, \boldsymbol{H})$ be the event that $\mathcal{A}$ succeeds in the hint-IMP-PA game on input an input from X and $\boldsymbol{H}$. Similarly, let $B(X, \boldsymbol{H})$ be the event that $\mathcal{B}$ succeeds in outputting a witness for $\tilde{R}$.

Fix a statement $x \in \mathcal{X}$ and hints $\boldsymbol{h} = (h_1, \ldots, h_q) \in \mathsf{HintSet}_x^q$.

$$\Pr\left[\, B(X,H) \;\middle|\; X = x, H = \boldsymbol{h} \right] \geq \Pr\left[\, A(X,H) \;\middle|\; X = x, H = \boldsymbol{h} \right] - \frac{1}{|\mathcal{C}|}$$

Then by linearity,

$$\begin{aligned}
\Pr\left[\, B(X,H) \right] &= \sum_{x,\boldsymbol{h}} \Pr\left[\, X = x, H = \boldsymbol{h} \right] \Pr\left[\, B(X,H) \;\middle|\; X = x, H = \boldsymbol{h} \right] \\
&\geq \sum_{x,\boldsymbol{h}} \Pr\left[\, X = x, H = \boldsymbol{h} \right] \left(\Pr\left[\, A(X,H) \;\middle|\; X = x, H = \boldsymbol{h} \right] - \frac{1}{|\mathcal{C}|} \right) \\
&= \Pr\left[\, A(X,H) \right] - \frac{1}{|\mathcal{C}|}.
\end{aligned}$$

Finally, the expected runtime of $\mathcal{B}$ is about the same as $\mathcal{E}$. □

Note that the above is not quite a reduction from the hard relation with hints $(\tilde{R}, \mathcal{H})$ to the hint-IMP-PA-security of Σ. In particular, the definition of a hard relation with hints is only with respect to PPT algorithms. However, the algorithm constructed is just an *expected* polynomial time algorithm. To finish the reduction, we convert it to a PPT algorithm in a standard way.

Lemma 3.3. *Let $\mathcal{A}$ be an algorithm that runs in expected time t with success probability ε. Then there exists an algorithm $\mathcal{B}$ that runs in time at most $2t/\varepsilon$ and succeeds with probability at least $\varepsilon/2$. In particular, if t and ε^{-1} are polynomial in λ, then $\mathcal{B}$ runs in polynomial time in λ and has non-negligible success probability.*

Proof. $\mathcal{B}$ runs $\mathcal{A}$ but times out after $2t/\varepsilon - 1$ steps. Let T be the random variable for the runtime of $\mathcal{A}$. By Markov's inequality,

$$\Pr\left[\, T \geq 2t/\varepsilon \right] \leq \frac{E[T]}{2t/\varepsilon} = \frac{\varepsilon}{2}.$$

Let $S_{\mathcal{A}}$ and $S_{\mathcal{B}}$ be the events that $\mathcal{A}$ and $\mathcal{B}$ succeeds, respectively.

$$\Pr\left[\, S_{\mathcal{B}} \right] = \Pr\left[\, S_{\mathcal{A}}, T < 2t/\varepsilon \right] \geq \Pr\left[\, S_{\mathcal{A}} \right] - \Pr\left[\, T \geq 2t/\varepsilon \right] \geq \varepsilon - \varepsilon/2 = \varepsilon/2.$$

□

In conclusion, we obtain a reduction from the hard relation with hints $(\tilde{R}, \mathcal{H})$ to the EUF-CMA security of $\mathsf{SIG}[\Sigma]$.

Theorem 1 (hint-rel reduces to EUF-CMA). *Let $(R, \mathcal{H})$ be a relation with hints. Let Σ be a Σ-protocol for the relation R that has challenge space $\mathcal{C}$ and is special-sound with respect to a soundness relation $\tilde{R}$. Additionally, let $\mathcal{S}$ be a $\mathcal{H}$-hint-assisted simulator for Σ.*

For any PPT algorithm $\mathcal{A}$ against the EUF-CMA of $\mathsf{SIG}[\Sigma]$, there exists a PPT algorithm $\mathcal{B}$ and an expected polynomial time algorithm $\mathcal{E}$ such that

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SIG}[\Sigma]}(\mathcal{A}) \leq (q+1) \cdot \left(\mathsf{Adv}^{\mathsf{hint\text{-}rel}}_{(\tilde{R},\mathcal{H})}(\mathcal{E}, s) + \mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma,\mathcal{H},\mathcal{S}}(\mathcal{B}, s) + \frac{1}{|\mathcal{C}|} \right) + (q+s+1)s \cdot \mathsf{MinEnt}(\Sigma),$$

where q and s are upper-bounds on the number of queries that $\mathcal{A}$ makes to RO *and* OSign*, respectively.*

4 Analyzing SQIsign in the Fiat–Shamir with Hint Framework

We now apply the framework introduced in the previous section to study the security of SQIsign.

Commitment min-entropy. We begin by analyzing the distribution of the commitment $D_{,}$. For every supersingular curve E, we define D^{mix}_E as the distribution on $j(\mathsf{Supersingular}_p)$ obtained by taking the codomain of a uniformly random cyclic isogeny $\varphi : E \to E'$ of degree N_{mix}. The commitment distribution is $D_{,} = D^{\mathsf{mix}}_{E_0}$ and $\Delta(D_{,}, S_j) \leq 1/(2\sqrt{p})$ by Proposition 2.1.

Lemma 4.1. $\mathsf{MinEnt}(\Sigma_{\mathsf{SQI}}) \leq p^{-1/2}$.

Proof. The commitment distribution $D_{,}$ is independent of the statement or witness. By the definition of statistical distance, $\mathsf{MinEnt}(\Sigma_{\mathsf{SQI}}) \leq \Delta(D_{,}, S_j) + \Pr\left[\mathsf{com}' = \mathsf{com} \;\middle|\; \mathsf{com}' \leftarrow S_j\right]$, for some commitment com. Then,

$$\Pr\left[\mathsf{com}' = \mathsf{com} \;\middle|\; \mathsf{com}' \leftarrow S_j\right] \leq \frac{12}{p-1} \leq \frac{1}{2\sqrt{p}},$$

using first that $|\operatorname{Aut}(E)| \geq 2$ for all $E \in \mathsf{Supersingular}_p$ and second that $p \geq 578$. We conclude using $\Delta(D_{,}, S_j) \leq 1/(2\sqrt{p})$. □

Special Soundness. While Σ_{SQI} is not special-sound with respect to the original relation R_{SQI}, [8] showed that it is special-sound with respect to OneEnd_p.

Experiment 2: Hint distribution $\mathcal{H}^{\mathsf{sim}}$ for SQIsign

$\underline{D_{\mathsf{Chall}}(E)}$:

1: $s \xleftarrow{\$} \{0, \ldots, 2^{e_{\mathsf{chl}}} - 1\}$.
2: $(P, Q) := \mathsf{DeterministicBasis}(E)$.
3: Compute the isogeny $\varphi : E \to E'$ with $\ker(\varphi) = \langle P + [s]Q \rangle$ exactly as Σ_{SQI} does for the challenge isogeny.
4: **return** s, φ.

$\underline{D_{\mathsf{StatTarget}}(E)}$:

1: Sample an isogeny $\varphi : E \to E'$ such that
   i E' is distributed according to the stationary distribution S on $\mathsf{Supersingular}_p$.
   ii The conditional distribution of φ given E' is uniform among isogenies $E \to E'$ of degree $< 2^{e_{\mathsf{rsp}}}$.
2: Write $\varphi = [m] \circ \varphi'$ with $m \in \mathbb{Z}$ and φ' cyclic.
3: **return** an efficient representation of φ'.

$\underline{D_{\mathsf{Uniflsog}}(E, d)}$:

1: Sample an isogeny $\varphi : E \to E'$ uniformly among the cyclic isogenies from E of degree d to curves in $\mathsf{Supersingular}_p$.
2: **return** an efficient representation of φ.

$\underline{\mathcal{H}^{\mathsf{sim}}_E}$:

1: $s, \varphi_1 \leftarrow D_{\mathsf{Chall}}(E)$, where $\varphi_1 : E \to E_1$.
2: $\varphi_2 \leftarrow D_{\mathsf{StatTarget}}(E_1)$, where $\varphi_2 : E_1 \to E_2$.
3: Write $\deg(\varphi_2) = 2^n d'$ with d' odd.
4: $\varphi_3 \leftarrow D_{\mathsf{Uniflsog}}(E_2, 2^{e_{\mathsf{rsp}}-n} - d')$, where $\varphi_3 : E_2 \to E_3$.
5: **return** $h = (s, \varphi_2, \varphi_3)$.

Lemma 4.2 ([8, Theorem 17])**.** *If $e_{\mathsf{chl}} + e_{\mathsf{rsp}} \leq e$, then Σ_{SQI} is special-sound with respect to the soundness relation*

$$R_{\mathsf{OneEnd}} = \left\{ ((\mathsf{pp}, A_{\mathsf{pk}}), \alpha) \;\middle|\; \begin{array}{c} \mathsf{pp} \text{ public parameters, } A_{\mathsf{pk}} \in \mathbb{F}_{p^2}, \\ E_{\mathsf{pk}} := E_{A_{\mathsf{pk}}} \in \mathsf{Supersingular}_p, \\ \alpha \in \mathrm{End}(E) \setminus \mathbb{Z} \text{ in efficient representation}, \\ \deg(\alpha) \leq p^4 \end{array} \right\}.$$

Hint-assisted wHVZK. We will prove that Σ_{SQI} is hint-assisted wHVZK with respect to the hint distribution $\mathcal{H}^{\mathsf{sim}}$ defined in Experiment 2. In essence, the hint provides the simulator with a response isogeny and auxiliary isogeny sampled from the correct distribution. Without knowledge of the endomorphism ring of

Algorithm 4: The hint-assisted simulator $\mathcal{S}_{\mathsf{SQI}}(\mathsf{pp}, A_{\mathsf{pk}}, h)$

Input: The statement $(\mathsf{pp}, A_{\mathsf{pk}})$ and a hint $h = (s, \widehat{\varphi_{\mathsf{rsp}}}, \varphi_{\mathsf{aux}}) \in \mathsf{HintSet}^{\mathsf{sim}}_{E_{\mathsf{pk}}}$ with $\widehat{\varphi_{\mathsf{rsp}}} : E_{\mathsf{chl}} \to E_{\mathsf{com}}$ and $\varphi_{\mathsf{aux}} : E_{\mathsf{com}} \to E^{\dagger}_{\mathsf{aux}}$.
Output: Transcript of Σ_{SQI}.

1: $, \coloneqq j(E_{\mathsf{com}})$ and $\mathsf{chl} \coloneqq s$.
2: $(P_{\mathsf{pk}}, Q_{\mathsf{pk}}) \coloneqq \mathsf{DeterministicBasis}(E_{\mathsf{pk}})$.
3: Compute $\varphi_{\mathsf{chl}} : E_{\mathsf{pk}} \to E_{\mathsf{chl}}$ with $\ker(\varphi_{\mathsf{chl}}) = \langle P_{\mathsf{pk}} + [s]Q_{\mathsf{pk}} \rangle$, exactly as Σ_{SQI} does for the challenge isogeny.
4: Compute the backtracking component of φ_{chl} and $\widehat{\varphi_{\mathsf{rsp}}}$ with Lemma 2.1, obtaining ψ_{bt} and $\widehat{\psi_{\mathsf{rsp}}}$ such that

$$\widehat{\varphi_{\mathsf{rsp}}} : E_{\mathsf{chl}} \xrightarrow{\psi_{\mathsf{bt}}} F \xrightarrow{\widehat{\psi_{\mathsf{rsp}}}} E_{\mathsf{com}} \qquad \text{and} \qquad \ker(\psi_{\mathsf{bt}}) = \ker(\widehat{\varphi_{\mathsf{chl}}}) \cap \ker(\widehat{\varphi_{\mathsf{rsp}}}).$$

5: Let $n_{\mathsf{bt}} \in \mathbb{Z}$ be such that $\deg(\psi_{\mathsf{bt}}) = 2^{n_{\mathsf{bt}}}$.
6: Let r' be the largest integer such that $2^{r'} | \deg(\psi_{\mathsf{rsp}})$.
7: Use Lemma 2.1 to compute efficient representations of ψ_{rsp} and $\widehat{\varphi_{\mathsf{aux}}}$.
8: Compute $\varphi'_{\mathsf{chl}} : E_{\mathsf{pk}} \to E'_{\mathsf{chl}}$ with $\ker(\varphi'_{\mathsf{chl}}) = \langle [2^{n_{\mathsf{bt}}}](P_{\mathsf{pk}} + [s]Q_{\mathsf{pk}}) \rangle$, as the verifier would.
9: Compute an isomorphism $\iota_{\mathsf{chl}} : F \to E'_{\mathsf{chl}}$.
10: $\varphi'_{\mathsf{rsp}} \coloneqq \iota_{\mathsf{chl}} \circ \psi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E'_{\mathsf{chl}}$.
11: $(P_{\mathsf{aux}}, Q_{\mathsf{aux}}) \coloneqq [2^{e-(e_{\mathsf{rsp}}-n_{\mathsf{bt}}+2)}] \cdot \mathsf{DeterministicBasis}(E^{\dagger}_{\mathsf{aux}})$.
12: $P_{\mathsf{chl}} \coloneqq [\deg(\varphi_{\mathsf{aux}})^{-1}]\varphi'_{\mathsf{rsp}} \circ \widehat{\varphi_{\mathsf{aux}}}(P_{\mathsf{aux}})$.
13: $Q_{\mathsf{chl}} \coloneqq [\deg(\varphi_{\mathsf{aux}})^{-1}]\varphi'_{\mathsf{rsp}} \circ \widehat{\varphi_{\mathsf{aux}}}(Q_{\mathsf{aux}})$.
14: **if** $-P_{\mathsf{chl}}$ is lexicographically smaller than P_{chl} **then**
15: $\quad P_{\mathsf{chl}}, Q_{\mathsf{chl}} \coloneqq -P_{\mathsf{chl}}, -Q_{\mathsf{chl}}$
16: $\mathsf{rsp} \coloneqq (n_{\mathsf{bt}}, r', E^{\dagger}_{\mathsf{aux}}, P_{\mathsf{chl}}, Q_{\mathsf{chl}})$.
17: **return** $(, , \mathsf{chl}, \mathsf{rsp})$.

E_{pk}, we only know how to efficiently sample random isogenies of *smooth* degree. Our $\mathcal{H}^{\mathsf{sim}}$-hint-assisted simulator is defined in Algorithm 4.

To show that Σ_{SQI} is $\mathcal{H}^{\mathsf{sim}}$-assisted wHVZK, we begin by comparing the distribution of real and simulated transcripts. The commitment $j(E_{\mathsf{com}})$ has the distribution $D_{,}$ in real transcripts and the stationary distribution S_j in simulated transcripts. By Proposition 2.1, these distributions are statistically close. The challenge is also identically distributed in simulated and real transcripts. What remains is to compare the responses $\mathsf{rsp} = (n_{\mathsf{bt}}, r', A^{\dagger}_{\mathsf{aux}}, P_{\mathsf{chl}}, Q_{\mathsf{chl}})$.

Lemma 4.3. *Let* $((\mathsf{pp}, A_{\mathsf{pk}}), I_{\mathsf{sk}}) \in R_{\mathsf{SQI}}$ *and let* $j_{\mathsf{com}} \in j(\mathsf{Supersingular}_p)$. *Consider transcripts for the statement* $(\mathsf{pp}, A_{\mathsf{pk}})$, $(j_{\mathsf{com}}, \mathsf{chl}, \mathsf{rsp})$ *with the commitment fixed to* j_{com}. *Then* $\deg(\varphi_{\mathsf{rsp}})$, n_{bt}, r', E'_{chl} *and* $E^{\dagger}_{\mathsf{aux}}$ *are identically distributed in real and simulated transcripts of this form.*

Proof. In the response algorithm in Algorithm 2, the ideal J is uniformly distributed among the equivalent ideals to $\overline{I_{\mathsf{com}}} \cdot I_{\mathsf{sk}} \cdot I_{\mathsf{chl}}$ of norm $< 2^{e_{\mathsf{rsp}}}$. Then, the response ideal I_{rsp} is the primitive component of J.

The simulator's response isogeny φ_{rsp} is the cyclic component of a uniformly random isogeny $E_{\mathsf{com}} \to E_{\mathsf{chl}}$ of norm $< 2^{e_{\mathsf{rsp}}}$. The ideal corresponding to φ_{rsp} depends on $j(E_{\mathsf{com}}) = j_{\mathsf{com}}$ but not on the representative E_{com}. Hence, the ideal has the same distribution as the prover's I_{rsp}. The values $\deg(\varphi_{\mathsf{rsp}})$ n_{bt} and r' are uniquely determined by the response ideal and the challenge, so their simulated distributions are the same as the real ones.

Fix a choice of $\deg(\varphi_{\mathsf{rsp}})$, n_{bt} and r' and write $\deg(\varphi_{\mathsf{rsp}}) = 2^n d'$ with d' odd. Given these values, the prover and simulator produce the same curve E'_{chl}, by computing $\varphi_{\mathsf{chl}} : E_{\mathsf{pk}} \to E'_{\mathsf{chl}}$ with $\ker(\varphi'_{\mathsf{chl}}) = \langle [2^{n_{\mathsf{bt}}}](P_{\mathsf{pk}} + [\mathsf{chl}]Q_{\mathsf{pk}}) \rangle$.

Let $d_{\mathsf{aux}} = 2^{e_{\mathsf{rsp}}-n} - d'$. In line 7 of the response algorithm, I''_{aux} is uniformly distributed among the primitive left $\mathcal{O}_0$-ideals of norm d_{aux}. Since the norm of I_{com} is coprime to d_{aux}, we can define the pushforward I_{aux} of I''_{aux} through I_{com}. It corresponds to the prover's auxiliary isogeny $\varphi_{\mathsf{aux}} : E_{\mathsf{com}} \to E_{\mathsf{aux}}$. The pushforward by I_{com} induces a bijection between the left $\mathcal{O}_0$ ideals of norm d_{aux} and the left $\mathcal{O}_{\mathsf{com}}$-ideals of norm d_{aux}. Hence, I_{aux} is uniformly distributed among the primitive left-$\mathcal{O}_{\mathsf{com}}$ ideals of norm d_{aux}. Given I_{aux}, the prover picks a uniformly random A-invariant $A^{\dagger}_{\mathsf{aux}}$ for the representative of the codomain.

On the other hand, the simulator's auxiliary isogeny $\varphi_{\mathsf{aux}} : E_{\mathsf{com}} \to E^{\dagger}_{\mathsf{aux}}$ is uniformly distributed among the cyclic isogenies from E_{com} of degree d_{aux} to curves in $\mathsf{Supersingular}_p$. Hence, the corresponding ideal has the same distribution as the prover's I_{aux}. Fix the j-invariant j_{aux} of the codomain. The number of cyclic isogenies $E_{\mathsf{com}} \to E_{\mathsf{aux}}$ of degree d_{aux} is the same for any representative E_{aux} with $j(E_{\mathsf{aux}}) = j_{\mathsf{aux}}$. Hence, given j_{aux}, the simulator's $E^{\dagger}_{\mathsf{aux}}$ is uniformly distributed among the representatives for j_{aux}. □

Finally, we compare the distribution of the points $P_{\mathsf{chl}}, Q_{\mathsf{chl}}$. It turns out that their distribution depends on the automorphism group of E'_{chl}.

Lemma 4.4. *Let* $((\mathsf{pp}, A_{\mathsf{pk}}), I_{\mathsf{sk}}) \in R_{\mathsf{SQI}}$ *and let* $j_{\mathsf{com}} \in j(\mathsf{Supersingular}_p)$. *Consider transcripts for the statement* $(\mathsf{pp}, A_{\mathsf{pk}})$ *with the commitment fixed to* j_{com} *and* $j(E'_{\mathsf{chl}}) \notin \{0, 1728\}$. *Then* P_{chl} *and* Q_{chl} *are identically distributed in real and simulated transcripts of this form.*

Proof. At line 20 in the response algorithm in Algorithm 2, we have

$$R_{\mathsf{chl}} = \iota_{\mathsf{chl}} \circ \varphi^{\mathsf{even}}_{\mathsf{rsp}} \circ \varphi^{\mathsf{odd}}_{\mathsf{rsp}}(P_{\mathsf{com}}), \qquad R_{\mathsf{aux}} = \iota_{\mathsf{aux}} \circ \varphi_{\mathsf{aux}}(P_{\mathsf{com}}),$$
$$S_{\mathsf{chl}} = \iota_{\mathsf{chl}} \circ \varphi^{\mathsf{even}}_{\mathsf{rsp}} \circ \varphi^{\mathsf{odd}}_{\mathsf{rsp}}(Q_{\mathsf{com}}), \qquad S_{\mathsf{aux}} = \iota_{\mathsf{aux}} \circ \varphi_{\mathsf{aux}}(Q_{\mathsf{com}}),$$

where $\iota_{\mathsf{chl}} : E^{\mathsf{odd}}_{\mathsf{rsp}} \to E'_{\mathsf{chl}}$ and $\iota_{\mathsf{aux}} : E_{\mathsf{aux}} \to E^{\dagger}_{\mathsf{aux}}$ are the isomorphisms computed. Since $\deg(\varphi_{\mathsf{aux}})$ is odd and $P_{\mathsf{com}}, Q_{\mathsf{com}} \in E_{\mathsf{com}}[2^e]$, $(P_{\mathsf{com}}, Q_{\mathsf{com}})$ is the image of $(R_{\mathsf{aux}}, S_{\mathsf{aux}})$ through $[\deg(\varphi_{\mathsf{aux}})^{-1}] \circ \widehat{\varphi_{\mathsf{aux}}} \circ \widehat{\iota_{\mathsf{aux}}}$. It follows that

$$R_{\mathsf{chl}} = [\deg(\varphi_{\mathsf{aux}})^{-1}] \circ \iota_{\mathsf{chl}} \circ \varphi^{\mathsf{even}}_{\mathsf{rsp}} \circ \varphi^{\mathsf{odd}}_{\mathsf{rsp}} \circ \widehat{\varphi_{\mathsf{aux}}} \circ \widehat{\iota_{\mathsf{aux}}}(R_{\mathsf{aux}}) \text{ and}$$
$$S_{\mathsf{chl}} = [\deg(\varphi_{\mathsf{aux}})^{-1}] \circ \iota_{\mathsf{chl}} \circ \varphi^{\mathsf{even}}_{\mathsf{rsp}} \circ \varphi^{\mathsf{odd}}_{\mathsf{rsp}} \circ \widehat{\varphi_{\mathsf{aux}}} \circ \widehat{\iota_{\mathsf{aux}}}(S_{\mathsf{aux}}).$$

After line 23 the same relationship holds for $(P_{\mathsf{chl}}, Q_{\mathsf{chl}})$ as the evaluation of $(P_{\mathsf{aux}}, Q_{\mathsf{aux}})$. Finally, the lines 24–25 makes a deterministic choice of sign for P_{chl}

and Q_{chl}. The simulator computes $P_{\mathsf{chl}}, Q_{\mathsf{chl}}$ in the same manner, by pushing $P_{\mathsf{aux}}, Q_{\mathsf{aux}}$ through $[\deg(\varphi_{\mathsf{aux}})^{-1}] \circ \varphi'_{\mathsf{rsp}} \circ \widehat{\varphi_{\mathsf{aux}}}$ and then choosing the sign in the same way as the prover.

In the proof of Lemma 4.3, we saw that E'_{chl}, $E^{\dagger}_{\mathsf{aux}}$ and the ideals corresponding to $\varphi_{\mathsf{rsp}}, \varphi_{\mathsf{aux}}$ and φ_{chl} all have the same real and simulated distribution. These values determine the isogeny $E^{\dagger}_{\mathsf{aux}} \to E'_{\mathsf{chl}}$, up to post-composition with automorphisms. When $j(E'_{\mathsf{chl}}) \notin \{0, 1728\}$, the only automorphisms of E'_{chl} are $[\pm 1]$ [26, Theorem III.10.1]. Then the automorphisms of E'_{chl} only change the sign of the evaluation of the deterministic basis $(P_{\mathsf{aux}}, Q_{\mathsf{aux}})$. If the prover and simulator use isogenies $E^{\dagger}_{\mathsf{aux}} \to E'_{\mathsf{chl}}$ that agree up to post-composition with automorphisms, they compute the same $P_{\mathsf{chl}}, Q_{\mathsf{chl}}$, because they pick the same sign. So in this case, P_{chl} and Q_{chl} have the same real and simulated distribution. □

The case when $j(E'_{\mathsf{chl}})$ is 0 or 1728 must be handled separately. In this case, the real distribution of $P_{\mathsf{chl}}, Q_{\mathsf{chl}}$ might be distinguishable from the simulated distribution. However, we argue, in the full version of the paper [2], that this case will only happen with negligible probability if the $\mathsf{EndRing}_p$ problem is hard.

Lemma 4.5. *Let* $((\mathsf{pp}, A_{\mathsf{pk}}), I_{\mathsf{sk}}) \in R_{\mathsf{SQI}}$. *Let* $J^{\mathsf{real}}_{\mathsf{chl}'}$ *and* $J^{\mathsf{sim}}_{\mathsf{chl}'}$ *be random variables for the distribution of* $j(E'_{\mathsf{chl}})$ *in real and simulated transcripts, respectively. There exists a PPT adversary* $\mathcal{B}$ *against the hard relation* R_{SQI} *such that*

$$\Pr\left[J^{\mathsf{real}}_{\mathsf{chl}'} \in \{0, 1728\}\right] \leq \mathsf{Adv}^{\mathsf{rel}}_{R_{\mathsf{SQI}}}(\mathcal{B}) \text{ and } \Pr\left[J^{\mathsf{sim}}_{\mathsf{chl}'} \in \{0, 1728\}\right] \leq \mathsf{Adv}^{\mathsf{rel}}_{R_{\mathsf{SQI}}}(\mathcal{B}).$$

We are now finally ready to prove that Σ_{SQI} is $\mathcal{H}^{\mathsf{sim}}$-hint-assisted wHVZK.

Lemma 4.6 (Computational hint-assisted wHVZK). *Let* $\mathcal{S}_{\mathsf{SQI}}$ *be the* $\mathcal{H}^{\mathsf{sim}}$*-hint-assisted simulator defined in Algorithm 4. For any* $q = \mathsf{poly}(\lambda)$ *and any PPT adversary* $\mathcal{A}$ *against the hint-assisted wHVZK of* Σ_{SQI} *with* q *hints, there exists a PPT algorithm* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma_{\mathsf{SQI}}, \mathcal{H}^{\mathsf{sim}}, \mathcal{S}_{\mathsf{SQI}}}(\mathcal{A}, q) \leq \mathsf{Adv}^{\mathsf{rel}}_{R_{\mathsf{SQI}}}(\mathcal{B}) + 2q \cdot \Delta(D_{,}, S_j).$$

Proof The distinguishing advantage of $\mathcal{A}$ is

$$\mathsf{Adv}^{\mathsf{hint\text{-}wHVZK}}_{\Sigma_{\mathsf{SQI}}, \mathcal{H}^{\mathsf{sim}}, \mathcal{S}_{\mathsf{SQI}}}(\mathcal{A}) = \left|\Pr\left[b^{\mathsf{real}} = 1\right] - \Pr\left[b^{\mathsf{sim}} = 1\right]\right|,$$

where $b^{\mathsf{real}} := \mathcal{A}(\mathsf{Real}_{\Sigma_{\mathsf{SQI}}}(1^{\lambda}, q))$ and $b^{\mathsf{sim}} := \mathcal{A}(\mathsf{HintSim}_{\Sigma_{\mathsf{SQI}}}(1^{\lambda}, q, \mathcal{S}_{\mathsf{SQI}}))$.

We begin with the commitment. It is a j-invariant in $V := j(\mathsf{Supersingular}_p)$, distributed as $D_{,}$ in real transcripts, and as S_j in simulated transcripts. $\mathcal{A}$ is given q independently sampled commitments from one of the distributions. When $\mathcal{A}$ gets real transcripts, let $\boldsymbol{J}^{\mathsf{real}}_{,} = \left(J^{\mathsf{real}}_{,,1}, \ldots, J^{\mathsf{real}}_{,,q}\right)$ be the random variable for the q commitments. Similarly, when $\mathcal{A}$ gets simulated transcripts, let $\boldsymbol{J}^{\mathsf{sim}}_{,} = \left(J^{\mathsf{sim}}_{,,1}, \ldots, J^{\mathsf{sim}}_{,,q}\right)$ be the random variable for the q commitments. For $\boldsymbol{j} \in V^q$, we let $p^{\mathsf{real}}_{\boldsymbol{j}} = \Pr\left[\boldsymbol{J}^{\mathsf{real}}_{,} = \boldsymbol{j}\right]$ and $p^{\mathsf{sim}}_{\boldsymbol{j}} = \Pr\left[\boldsymbol{J}^{\mathsf{sim}}_{,} = \boldsymbol{j}\right]$. Using the statistical distance

between $D_{,}$ and S_j,

$$\begin{aligned}
\Pr\left[b^{\mathsf{real}}=1\right] &= \sum_{\boldsymbol{j}\in V^q} p_{\boldsymbol{j}}^{\mathsf{real}} \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&= \sum_{\boldsymbol{j}\in V^q} \left(p_{\boldsymbol{j}}^{\mathsf{real}} - p_{\boldsymbol{j}}^{\mathsf{sim}} + p_{\boldsymbol{j}}^{\mathsf{sim}}\right) \cdot \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&\leq \sum_{\boldsymbol{j}\in V^q} \left(\left|p_{\boldsymbol{j}}^{\mathsf{real}} - p_{\boldsymbol{j}}^{\mathsf{sim}}\right| + p_{\boldsymbol{j}}^{\mathsf{sim}}\right) \cdot \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&\leq \sum_{\boldsymbol{j}\in V^q} \left|p_{\boldsymbol{j}}^{\mathsf{real}} - p_{\boldsymbol{j}}^{\mathsf{sim}}\right| + \sum_{\boldsymbol{j}\in V^q} p_{\boldsymbol{j}}^{\mathsf{sim}} \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&= 2\Delta(\boldsymbol{J}_{,}^{\mathsf{real}}, \boldsymbol{J}_{,}^{\mathsf{sim}}) + \sum_{\boldsymbol{j}\in V^q} p_{\boldsymbol{j}}^{\mathsf{sim}} \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&\leq 2q\Delta(D_{,}, S_j) + \sum_{\boldsymbol{j}\in V^q} p_{\boldsymbol{j}}^{\mathsf{sim}} \Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right],
\end{aligned} \tag{1}$$

where the last step uses that the q transcripts have been sampled independently.

Next, we focus on $\Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right]$. It is the probability that $\mathcal{A}$ outputs 1 when it is given real transcripts with $\boldsymbol{j}$ as the commitments. When the commitments are fixed, we have seen in Lemma 4.3 and Lemma 4.4 that real and simulated transcripts are identically distributed, unless $j(E'_{\mathsf{chl}}) \in \{0, 1728\}$.

When $\mathcal{A}$ is given real transcripts, let G^{real} be the "good" event that all of the transcripts have $j(E'_{\mathsf{chl}}) \notin \{0, 1728\}$. Let G^{sim} be the corresponding event for the simulated transcripts. By Lemma 4.3, when the commitment is fixed, $j(E'_{\mathsf{chl}})$ has the same distribution in real and simulated transcripts. Hence, for all $\boldsymbol{j} \in V^q$,

$$\Pr\left[G^{\mathsf{real}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] = \Pr\left[G^{\mathsf{sim}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{sim}}=\boldsymbol{j}\right].$$

Furthermore, given that the good event has occurred, real and simulated transcripts are identically distributed, meaning that

$$\Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}, G^{\mathsf{real}}\right] = \Pr\left[b^{\mathsf{sim}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{sim}}=\boldsymbol{j}, G^{\mathsf{sim}}\right].$$

With these observations, we obtain that

$$\begin{aligned}
&\Pr\left[b^{\mathsf{real}}=1 \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&= \Pr\left[b^{\mathsf{real}}=1, G^{\mathsf{real}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] + \Pr\left[b^{\mathsf{real}}=1, \neg G^{\mathsf{real}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&\leq \Pr\left[b^{\mathsf{real}}=1, G^{\mathsf{real}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] + \Pr\left[\neg G^{\mathsf{real}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{real}}=\boldsymbol{j}\right] \\
&= \Pr\left[b^{\mathsf{sim}}=1, G^{\mathsf{sim}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{sim}}=\boldsymbol{j}\right] + \Pr\left[\neg G^{\mathsf{sim}} \;\middle|\; \boldsymbol{J}_{,}^{\mathsf{sim}}=\boldsymbol{j}\right].
\end{aligned}$$

Combining this with (1), we get that

$$\begin{aligned}
\Pr\left[b^{\mathsf{real}}=1\right] &\leq 2q\Delta(D_{,}, S_j) + \Pr\left[b^{\mathsf{sim}}=1, G^{\mathsf{sim}}\right] + \Pr\left[\neg G^{\mathsf{sim}}\right] \\
&\leq 2q\Delta(D_{,}, S_j) + \Pr\left[b^{\mathsf{sim}}=1\right] + \Pr\left[\neg G^{\mathsf{sim}}\right].
\end{aligned}$$

What remains is to upper bound the probability that G^{sim} does not occur, i.e. the event that one of the q simulated transcripts has $j(E'_{\mathsf{chl}}) \in \{0, 1728\}$. For a single transcript, the probability can be upper bounded by the advantage of a PPT adversary $\mathcal{N}$ against the relation R_{SQI}, by Lemma 4.5. $\mathcal{N}$ first perfectly simulates the challenge isogeny, and then tries to use it to compute a witness for the statement. Consider the adversary $\mathcal{B}$ that runs $\mathcal{N}$ q times with input E_{pk}, using a fresh random tape each time. Since $q = \mathsf{poly}(\lambda)$, $\mathcal{B}$ is PPT. Furthermore,

$$\Pr\left[\neg G^{\mathsf{sim}}\right] \leq \mathsf{Adv}^{\mathsf{rel}}_{R_{\mathsf{SQI}}}(\mathcal{B}).$$

We conclude that

$$\Pr\left[b^{\mathsf{real}} = 1\right] - \Pr\left[b^{\mathsf{sim}} = 1\right] \leq 2q \cdot \Delta(D_{,}, S_j) + \mathsf{Adv}^{\mathsf{rel}}_{R_{\mathsf{SQI}}}(\mathcal{B}).$$

By a symmetric argument, $\Pr\left[b^{\mathsf{sim}} = 1\right] - \Pr\left[b^{\mathsf{real}} = 1\right]$ has the same bound. □

We have shown that Σ_{SQI} has the properties required to apply the framework of Sect. 3. It has high commitment min-entropy, is $\mathcal{H}^{\mathsf{sim}}$-hint-assisted wHVZK, is special-sound with respect to the soundness relation R_{OneEnd} and has an exponentially large challenge space in λ. By Theorem 1, we obtain a reduction from the relation R_{OneEnd} with $\mathcal{H}^{\mathsf{sim}}$-hints to the EUF-CMA of $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$.

Theorem 2. *For any PPT algorithm $\mathcal{A}$ against the* EUF-CMA *of* $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$*, there exists an expected polynomial time algorithm $\mathcal{E}$ with*

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]}(\mathcal{A}) \leq (q+1) \cdot \left(2 \cdot \mathsf{Adv}^{\mathsf{hint\text{-}rel}}_{(R_{\mathsf{OneEnd}}, \mathcal{H}^{\mathsf{sim}})}(\mathcal{E}, s) + 2^{-e_{\mathsf{chl}}}\right) + \frac{(2q+s+2)s}{\sqrt{p}},$$

where q and s are upper bounds on the number of queries that $\mathcal{A}$ makes to RO *and* OSign*, respectively.*

5 Reducing Hint-EndRing to the EUF-CMA of SQIsign

Without hints, [22] reduced the $\mathsf{EndRing}_p$problem to the OneEnd_pproblem. In this section, our goal is to provide a similar reduction with hints. For this, we introduce a new hint distribution $\mathcal{H}^{\mathsf{unif}}$ for SQIsign. $\mathcal{H}^{\mathsf{unif}}$ is less structured and arguably more natural than $\mathcal{H}^{\mathsf{sim}}$. Additionally, hints from $\mathcal{H}^{\mathsf{unif}}$ are *pushable*. This means that given a 2^n-isogeny $\sigma : E \to E'$ and a hint $h \leftarrow \mathcal{H}^{\mathsf{unif}}_E$ for E, we can push it through σ to get a hint for E' distributed according to $\mathcal{H}^{\mathsf{unif}}_{E'}$. With this property, the OneEnd_pproblem with $\mathcal{H}^{\mathsf{unif}}$-hints is random self-reducible, and we obtain a reduction to it from the $\mathsf{EndRing}_p$problem with $\mathcal{H}^{\mathsf{unif}}$-hints. To argue that this new hint-EndRing problem can be reduced to the EUF-CMA of SQIsign, we introduce a new indistinguishability assumption.

Algorithm 5: The pushable hint distribution

$\underline{\mathcal{H}_E^{\mathsf{unif}}}$:

1: Sample an integer d from a weighted distribution on the interval $[1, 2^{e_{\mathsf{rsp}}}]$ where each integer n, with prime factorization $n = \prod_{i=1}^{t} p_i^{e_i}$, has weight $\prod_{i=1}^{t}(p_i + 1)^{e_i}$.
2: Sample an isogeny $\psi_1' : E \to E_1'$ uniformly among the (possibly non-cyclic) isogenies from E of degree d.
3: Write $\psi_1 : E \to E_1$ for the cyclic component of ψ_1'.
4: Write $\deg\psi_1 = 2^n d'$ with d' odd.
5: Sample an isogeny $\psi_2 : E_1 \to E_2$ uniformly among the cyclic isogenies from E_1 of degree $2^{e_{\mathsf{rsp}}-n} - d'$.
6: **return** $h = (\psi_1, \psi_2)$.

Algorithm 6: $\mathsf{PushHint}(E, h, \sigma)$

Input: $E \in \mathsf{Supersingular}_p$,
$h = (\psi_1, \psi_2) \in \mathsf{HintSet}_E^{\mathsf{unif}}$ with $\psi_1 : E \to E_1$ and $\psi_2 : E_1 \to E_2$,
cyclic 2^k-isogeny $\sigma : E \to E'$ in efficient representation.
Output: $h' \in \mathsf{HintSet}_{E'}^{\mathsf{unif}}$

1: Write ψ for the composition $\psi = \psi_2 \circ \psi_1$.
2: Write $\deg(\psi) = 2^n d_{\mathsf{odd}}$ with d_{odd} odd.
3: Compute the pushforward $\psi_{\mathsf{odd}}' : E' \to E_1'$ of ψ_{odd} by τ.
4: Sample $\psi_{2^n}' : E_1' \to E_2'$ as a random cyclic 2^n-isogeny from E_1'.
5: Let $\psi' = \psi_{2^n}' \circ \psi_{\mathsf{odd}}'$.
6: Write ψ' for the composition $\psi' = \psi_2' \circ \psi_1'$ where $\deg\psi_i' = \deg\psi_i$ for $i \in \{1, 2\}$.
7: **return** $h' = (\psi_1', \psi_2')$.

5.1 The Pushable Hint Distribution

We introduce a new hint distribution $\mathcal{H}^{\mathsf{unif}}$: rather than sampling a random curve and generating a connecting isogeny, the new hint distribution $\mathcal{H}_E^{\mathsf{unif}}$ samples random isogenies directly from E, as defined in Experiment 5. The main property of the new distribution is that, unlike the previous hint distribution $\mathcal{H}^{\mathsf{sim}}$, it is pushable. We push hints using Algorithm 6. We prove that the output of Algorithm 6 is distributed as $\mathcal{H}_{E'}^{\mathsf{unif}}$ in the full version of this paper [2].

Lemma 5.1. *Let $E \in \mathsf{Supersingular}_p$, let $k \in \mathbb{N}$ and let $\sigma : E \to E'$ be a cyclic 2^k-isogeny in efficient representation. If $h \leftarrow \mathcal{H}_E^{\mathsf{unif}}$, then $\mathsf{PushHint}(E, h, \sigma)$ is distributed according to $\mathcal{H}_{E'}^{\mathsf{unif}}$.*

By relying on the pushing algorithm (Algorithm 6), we can use a hint from $\mathcal{H}^{\mathsf{unif}}$ to generate something that looks like a hint from $\mathcal{H}^{\mathsf{sim}}$. Formally, we consider the problem of distinguishing between the two distributions in Experi-

Experiment 3: Hint distinguishing

$\mathsf{RealHints}(1^\lambda, q)$:

1: $(E, I) \leftarrow \mathsf{Gen}_{R_{\mathsf{SQI}}}(1^\lambda)$
2: **for** $i = 1$ **to** q **do**
3: $\quad h_i \leftarrow \mathcal{H}_E^{\mathsf{sim}}$
4: **return** $(E, h_1, \ldots, h_q)$

$\mathsf{PushedHints}(1^\lambda, q)$:

1: $(E, I) \leftarrow \mathsf{Gen}_{R_{\mathsf{SQI}}}(1^\lambda)$
2: **for** $i = 1$ **to** q **do**
3: $\quad (\psi_1, \psi_2) \leftarrow \mathcal{H}_E^{\mathsf{unif}}$
4: $\quad (s, \varphi) \leftarrow D_{\mathsf{Chall}}(E)$ // see Experiment 2
5: $\quad (\psi_1', \psi_2') \leftarrow \mathsf{PushHint}(E, (\psi_1, \psi_2), \varphi)$
6: $\quad h_i \coloneqq (s, \psi_1', \psi_2')$
7: **return** $(E, h_1, \ldots, h_q)$

ment 3. For $q = \mathsf{poly}(\lambda)$, we refer to this as the q-hint distinguishing problem (q-hint-dist).

Problem 3 (q-hint-dist)**.** *Let* $(E, h_1, \ldots, h_q)$ *be sampled with probability 1/2 from* $\mathsf{RealHints}(1^\lambda, q)$ *and with probability 1/2 from* $\mathsf{PushedHints}(1^\lambda, q)$*, where* $\mathsf{RealHints}(1^\lambda, q)$ *and* $\mathsf{PushedHints}(1^\lambda, q)$ *are defined in Experiment 3. Given* $(E, h_1, \ldots, h_q)$*, distinguish between the two distributions.*

For an algorithm $\mathcal{A}$, we let

$$\mathsf{Adv}^{\mathsf{hint\text{-}dist}}(\mathcal{A}, q) \coloneqq \mathsf{Adv}^{\mathsf{dist}}\left[\mathsf{RealHints}(1^\lambda, q), \mathsf{PushedHints}(1^\lambda, q)\right](\mathcal{A})\,.$$

Remark 5.1. We expect q-hint-dist to be computationally hard, following a similar argument on the heuristical equivalence of two oracles in SQIsign2D-West [8, Sec. 5.2]. The two hints distributions provide a representation of three isogenies $\varphi_1 : E \to E_1$, $\varphi_2 : E_1 \to E_2$, and $\varphi_3 : E_2 \to E_3$. The first isogeny φ_1 is sampled according to the same distribution in both games, thus E, E_1 and the isogeny φ_1 cannot provide any distinguishing information. The same is true for the third isogeny φ_3: fixed a starting curve E_2, the isogeny φ_3 is sampled according to the same distribution in both games. Thus, we focus on the second isogeny: in $\mathsf{RealHints}(1^\lambda, q)$, the isogeny φ_2 is uniformly distributed among the isogenies between E_1 and E_2; by rejection sampling, the same is true in $\mathsf{PushedHints}(1^\lambda, q)$. Hence, the only distinguishing factor is the distribution of the curve E_2: in $\mathsf{RealHints}(1^\lambda, q)$ it is distributed according to the stationary distribution, while in $\mathsf{PushedHints}(1^\lambda, q)$ it is the codomain of a random isogeny φ_2 from E_1 of bounded degree. If the isogeny φ_2 was sufficiently long, the statistical distance between the curves E_2 produced by the two games would become negligible; in our case, the bound on the degree of φ_2 prevents E_2 from being close to stationary. However, since the bound on the degree is exponential in λ, we still expect the distinguishing problem to be computationally hard.

5.2 The Reduction from Hint-OneEnd

Problem 4 (q-**hint-OneEnd**$_p$)**.** *Given a curve E sampled from the stationary distribution S on* $\mathsf{Supersingular}_p$ *and q hints $h_1, \ldots, h_q \leftarrow \mathcal{H}_E^{\mathsf{unif}}$, find an endomorphism in* $\mathrm{End}(E) \setminus \mathbb{Z}$ *in efficient representation.*

For an algorithm $\mathcal{A}$, we write $\mathsf{Adv}^{\mathsf{hint\text{-}OneEnd}_p}(\mathcal{A}, q)$ for the probability that it solves $q\mathsf{hint\text{-}OneEnd}_p$. We obtain a reduction from $q\mathsf{hint\text{-}OneEnd}_p$ by replacing the hint distribution in Theorem 2 with $\mathcal{H}^{\mathsf{unif}}$.

Theorem 3. *For any PPT algorithm $\mathcal{A}$ against the* EUF-CMA *of* $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$*, there exist expected polynomial time algorithms $\mathcal{B}$ and $\mathcal{D}$ with*

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]}(\mathcal{A}) \leq (q+1) \cdot \left(2 \cdot \mathsf{Adv}^{\mathsf{hint\text{-}OneEnd}_p}(\mathcal{B}, s) + 2 \cdot \mathsf{Adv}^{\mathsf{hint\text{-}dist}}(\mathcal{D}, s) + 2^{-e_{\mathsf{chl}}}\right) + \frac{2qs + s^2 + 2s + q + 1}{\sqrt{p}},$$

where q and s are upper bounds on the number of queries that $\mathcal{A}$ makes to RO *and* OSign*, respectively.*

The proof of Theorem 3 is in the full version of this paper [2]. An important property of the OneEnd_p problem is that it is a random self-reducible. Since $\mathcal{H}^{\mathsf{unif}}$-hints are pushable, we can show that $q\mathsf{hint\text{-}OneEnd}_p$ retains this property.

Lemma 5.2. *Let $\mathcal{A}$ be an algorithm for $q\mathsf{hint\text{-}OneEnd}_p$ with advantage ε and outputs of degree at most d. Then we can construct an algorithm $\mathcal{A}'$ such that:*

1. *For any curve $E \in \mathsf{Supersingular}_p$, it solves $q\mathsf{hint\text{-}OneEnd}_p$ for E with probability in $[\varepsilon - \frac{\log p}{p}, \varepsilon + \frac{\log p}{p}]$.*
2. *It runs $\mathcal{A}$ once. The rest runs in polynomial time in $\log p$, $\log d$ and q.*
3. *Its output has degree at most $2^{6\lceil \log p \rceil} \cdot d$.*

Proof (sketch). $\mathcal{A}'$ samples $\sigma : E \to E'$ from a random non-backtracking 2-isogeny walk of length $3\lceil \log p \rceil$, pushes the hints through σ, and runs $\mathcal{A}$ on E' and the pushed hints, trying to obtain $\alpha \in \mathrm{End}(E') \setminus \mathbb{Z}$. If so, it outputs $\widehat{\sigma} \circ \alpha \circ \sigma$. For the full proof, the see the full version of this paper [2]. □

5.3 The Classical Reduction from Hint-EndRing

Problem 5 (q-**hint-EndRing**$_p$)**.** *Given a curve E sampled from the stationary distribution S on* $\mathsf{Supersingular}_p$ *and q hints $h_1, \ldots, h_q \leftarrow \mathcal{H}_E^{\mathsf{unif}}$, find four endomorphisms in efficient representation that form a basis of* $\mathrm{End}(E)$*.*

For an algorithm $\mathcal{A}$, we let $\mathsf{Adv}^{\mathsf{hint\text{-}EndRing}_p}(\mathcal{A}, q)$ denote the probability that $\mathcal{A}$ succeeds in solving q-$\mathsf{hint\text{-}EndRing}_p$.

Without hints, [22] proved that an oracle for OneEnd_pcan be used to construct an efficient algorithm for $\mathsf{EndRing}_p$.

Lemma 5.3 ([22]). *Let* OEnd *be an oracle for* OneEnd_p*, that when queried on a curve* $E \in \mathsf{Supersingular}_p$ *outputs an endomorphism* $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ *of degree at most* d*. Then there is an algorithm* $\mathcal{A}$ *that, on input* $E \in \mathsf{Supersingular}_p$ *and given query access to the oracle* OEnd*, outputs a basis for* $\mathrm{End}(E)$ *in efficient representation.* $\mathcal{A}$ *runs in expected time* $\mathsf{poly}(\log p,\ \log d)$*, counting each call to* OEnd *as a single step.*

By inspecting the proof in [22], we obtain the following in the full version of this paper [2]. The runtime loss is polynomial in $\log p$, but concretely very large.

Corollary 5.1. *The runtime of* $\mathcal{A}$ *in Lemma 5.3 is* $\mathsf{poly}(\log p, \log d)$ *times the number of calls it makes to* OEnd*. In expectation, the number of calls is*

$$t_{\mathsf{OneEnd}}(\log p, \log d) < 2^{94} \cdot (\log(p) + \log(d)/30)^{13}.$$

We will show that with the pushable hint distribution $\mathcal{H}^{\mathsf{unif}}$, we can reduce $\mathsf{hint\text{-}EndRing}_p$ to $\mathsf{hint\text{-}OneEnd}_p$ in the same manner. We assume throughout that $q, \log d = \mathsf{poly}(\log p)$. In the reduction, we consider several kinds of oracles.

- For each $E \in \mathsf{Supersingular}_p$, OHint_E is an oracle that when queried outputs a fresh hint sampled from $\mathcal{H}^{\mathsf{unif}}_E$.
- For each $E \in \mathsf{Supersingular}_p$, $\mathsf{OEnd1}_{E,d}$ is an oracle that, given a 2^k-isogeny $\sigma : E \to E'$ in efficient representation for some k and $E' \in \mathsf{Supersingular}_p$, outputs a non-scalar endomorphism of E' of degree at most d.
- $\mathsf{OEnd2}_{q,d,\varepsilon}$ is an oracle which, given a curve $E \in \mathsf{Supersingular}_p$ and q hints $h_1, \ldots, h_q \leftarrow \mathcal{H}^{\mathsf{unif}}_E$, outputs a non-scalar endomorphism of E of degree at most d, with probability in $[\varepsilon - \frac{\log(p)}{p}, \varepsilon + \frac{\log(p)}{p}]$.

The oracles will represent the parts we have not yet implemented. In the runtime analysis, each call to an oracle counts as a single step.

Lemma 5.4. *There is an algorithm* $\mathcal{A}$*, which on input a curve* $E \in \mathsf{Supersingular}_p$ *and given query access to the oracle* $\mathsf{OEnd1}_{E,d}$*, computes* $\mathrm{End}(E)$*. Its runtime is* $\mathsf{poly}(\log p)$ *times the number of calls it makes to* $\mathsf{OEnd1}_{E,d}$*. In expectation, the number of times it calls* $\mathsf{OEnd1}_{E,d}$ *is* $t_{\mathsf{OneEnd}}(\log p, \log d)$*.*

Proof. We follow the reduction from $\mathsf{EndRing}_p$to OneEnd_pin [22]. We only need to implement their "rich oracle" $\mathsf{RICH}^{\mathcal{O}}$ with parameter $k = \mathsf{poly}(\log p)$ [22, Algorithm 1]. We implement it as follows.

1. Sample a 2^k-isogeny $\sigma : E \to E'$ by a random non-backtracking walk.
2. $\alpha \leftarrow \mathsf{OEnd1}_{E,d}(\sigma)$. (In the second stage of the reduction, reduce α.)
3. Return $\widehat{\sigma} \circ \alpha \circ \sigma$.

The expected number of calls to $\mathsf{OEnd1}_{E,d}$ is the expected number of calls to the OneEnd_poracle in the reduction in [22]. The runtime follows by Corollary 5.1. □

When ε is large enough, we implement $\mathsf{OEnd1}_{E,d}$ using OHint_E and $\mathsf{OEnd2}_{q,d,\varepsilon}$.

Lemma 5.5. *Assume $\varepsilon \geq 2\log(p)/p$. There is an algorithm $\mathcal{B}$, which on input a 2^k-isogeny $\sigma : E \to E'$ with $E, E' \in \mathsf{Supersingular}_p$, and given query-access to the oracles $\mathsf{OEnd2}_{q,d,\varepsilon}$ and OHint_E, has the following properties.*

1. *It outputs a non-scalar endomorphism of E' of degree at most d.*
2. *Its runtime is $k \cdot \mathsf{poly}(\log p)$ multiplied by the number of calls to $\mathsf{OEnd2}_{q,d,\varepsilon}$.*
3. *In expectation, it calls $\mathsf{OEnd2}_{q,d,\varepsilon}$ at most $2/\varepsilon$ times.*
4. *For every call to $\mathsf{OEnd2}_{q,d,\varepsilon}$, it makes q calls to OHint_E.*

Proof. On input $\sigma : E \to E'$, $\mathcal{B}$ follows these steps:

1. Sample $h_i \leftarrow \mathsf{OHint}_E$ for $i = 1, \ldots, q$.
2. $h'_i \leftarrow \mathsf{PushHint}(E, h_i, \sigma)$ for $i = 1, \ldots, q$.
3. $\alpha \leftarrow \mathsf{OEnd2}_{q,d,\varepsilon}(E', h'_1, \ldots, h'_q)$.
4. If $\alpha \in \mathbb{Z}$, go back to step 1. Else, output α.

Each iteration of the loop is an independent trial that succeeds with probability at least $\varepsilon - \log(p)/p \geq \varepsilon - \varepsilon/2 = \varepsilon/2$. □

Combing the two previous results, we obtain the following.

Corollary 5.2. *Assume $\varepsilon \geq 2\log(p)/p$. There exists an algorithm $\mathcal{D}$, which on input a curve $E \in \mathsf{Supersingular}_p$, and given query access to OHint_E and $\mathsf{OEnd2}_{q,d,\varepsilon}$, computes $\mathrm{End}(E)$. It has the following properties.*

1. *Its runtime is $\mathsf{poly}(\log p)$ multiplied by the number of times it calls $\mathsf{OEnd2}_{q,d,\varepsilon}$.*
2. *In expectation, it calls $\mathsf{OEnd2}_{q,d,\varepsilon}$ at most $2t_{\mathsf{OneEnd}}(\log p, \log d)/\varepsilon$ times.*
3. *For every call to $\mathsf{OEnd2}_{q,d,\varepsilon}$, it makes q calls to OHint_E.*

When we have an algorithm for $q$hint-OneEnd$_p$ with non-negligible advantage, we can convert it to an algorithm for s-hint-EndRing$_p$, without any oracles.

Lemma 5.6. *Let $\mathcal{A}$ be an expected polynomial time algorithm for $q$hint-OneEnd$_p$ with advantage $\varepsilon \geq 2\log(p)/p$ and with outputs of degree at most d. Let*

$$s \coloneqq 4q \cdot t_{\mathsf{OneEnd}}(\log p, \log d + 6\lceil \log p \rceil)/\varepsilon\,.$$

Then there exists an algorithm $\mathcal{B}$ for s-hint-EndRing$_p$, running in expected time $s \cdot \mathsf{poly}(\log p)$, with advantage at least $1/2$.

Proof. Let $\mathcal{D}$ be the oracle-algorithm from Corollary 5.2 with the degree bound $d' \coloneqq 2^{6\lceil \log p \rceil} \cdot d$. We will first convert $\mathcal{D}$ to an algorithm with bounded worst-case running time and then instantiate its oracles.

Recall that $\mathcal{D}$ succeeds with probability 1 and has a runtime that is $\mathsf{poly}(\log p)$ multiplied by the number of times it calls $\mathsf{OEnd2}_{q,d',\varepsilon}$. We will view the number of calls to this oracle as the runtime, and apply Lemma 3.3. In expectation, $\mathcal{D}$ makes $s/2$ calls to $\mathsf{OEnd2}_{q,d',\varepsilon}$. The corollary tells us that if we time out $\mathcal{D}$ after s calls to $\mathsf{OEnd2}_{q,d',\varepsilon}$, it still succeeds with probability at least $1/2$. Denote the algorithm that times out by $\mathcal{N}$. Its runtime is at most $s \cdot \mathsf{poly}(\log p)$.

Next, we instantiate the oracles of $\mathcal{N}$, to get an algorithm $\mathcal{B}$ for s-hint-EndRing$_p$. We implement OHint_E simply by answering the ith query with the ith hint h_i. We implement $\mathsf{OEnd2}_{q,d',\varepsilon}$ using $\mathcal{A}'$, the algorithm we obtain from the worst-case to average-case reduction in Lemma 5.2 with $\mathcal{A}$. It runs in expected time $\mathsf{poly}(\log p)$, with advantage in $[\varepsilon - \frac{\log p}{p}, \varepsilon + \frac{\log p}{p}]$. Its output has degree at most d'.

Composing the algorithm $\mathcal{A}'$ running in expected polynomial time with the oracle-algorithm $\mathcal{N}$ running in time $s \cdot \mathsf{poly}(\log p)$, we get that $\mathcal{B}$ runs in expected time $s \cdot \mathsf{poly}(\log p)$. Since $\mathcal{A}'$ always succeeds, $\mathcal{B}$ has the same advantage as $\mathcal{N}$. □

We conclude that if q-hint-EndRing$_p$and q-hint-dist are computationally hard problems, then $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$ is EUF-CMA-secure in the ROM. Our reduction inherits the non-tightness from [22]. The proof combines the previous results and can be found in the full version of this paper [2].

Theorem 4. *For any PPT algorithm $\mathcal{A}$ against the* EUF-CMA *of* $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$*, there are expected polynomial time algorithms $\mathcal{B}$ and $\mathcal{D}$ with*

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]}(\mathcal{A}) \leq (q+1) \cdot \left(2 \cdot \mathsf{Adv}^{\mathsf{hint\text{-}OneEnd}_p}(\mathcal{B}, s) + 2 \cdot \mathsf{Adv}^{\mathsf{hint\text{-}dist}}(\mathcal{D}, s) + 2^{-e_{\mathsf{chl}}}\right) + \frac{2qs + s^2 + 2s + q + 1}{\sqrt{p}},$$

where q and s are upper bounds on the number of queries that $\mathcal{A}$ makes to RO *and* OSign*, respectively. Whenever $\mathcal{B}$ has advantage $\varepsilon_{\mathcal{B}} \geq 2\log(p)/p$, there is an algorithm $\mathcal{E}$ for t-hint-EndRing$_p$, running in expected time $\mathsf{poly}(\log p)/\varepsilon_{\mathcal{B}}$, with*

$$t = 2^{102} \lceil \log p \rceil^{13} \cdot s/\varepsilon_{\mathcal{B}} \quad \text{and} \quad \mathsf{Adv}^{\mathsf{hint\text{-}EndRing}_p}(\mathcal{E}, t) \geq 1/2.$$

5.4 The Quantum Reduction from Hint-EndRing

We can obtain a much tighter *quantum* reduction from hint-EndRing$_p$ to hint-OneEnd$_p$. A serious source of complexity in the reduction of [22] arises from the possibility that a OneEnd$_p$oracle might produce endomorphisms with hard-to-factor discriminants. Without this obstacle, several steps of the reduction become redundant. We prove the following theorem in the full version of this paper [2].

Theorem 5. *Let* OEnd *be an oracle for the* OneEnd$_p$ *problem with outputs of degree at most d, and* OFactor *an oracle for integer factorization. Then there exists a three-stage algorithm for* EndRing$_p$ *which runs in expected time* $\mathsf{poly}(\log p, \log d)$*. The first and third stage each call* OEnd *in expectation 12 times. The second stage makes a single call to* OFactor *and runs in polynomial time.*

With Shor's algorithm [25], the second stage can be implemented by a quantum reduction. On the other hand, with a classical algorithm for hint-OneEnd$_p$,

the first and third stage can remain classical in the reduction to $\mathsf{hint\text{-}EndRing}_p$. Hence, we can apply our classical reduction separately for the first and third stage.

Theorem 6. *For any PPT algorithm $\mathcal{A}$ against the* EUF-CMA *of* $\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]$*, there are expected polynomial time algorithms $\mathcal{B}$ and $\mathcal{D}$ with*

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{SIG}[\Sigma_{\mathsf{SQI}}]}(\mathcal{A}) \leq (q+1)\cdot\left(2\cdot\mathsf{Adv}^{\mathsf{hint\text{-}OneEnd}_p}(\mathcal{B},s)+2\cdot\mathsf{Adv}^{\mathsf{hint\text{-}dist}}(\mathcal{D},s)+2^{-e_{\mathsf{chl}}}\right) + \frac{2qs+s^2+2s+q+1}{\sqrt{p}},$$

where q and s are upper bounds on the number of queries that $\mathcal{A}$ makes to RO *and* OSign*, respectively. Whenever $\mathcal{B}$ has advantage $\varepsilon_{\mathcal{B}} \geq 2\log(p)/p$, there is a quantum algorithm $\mathcal{E}$ for t-$\mathsf{hint\text{-}EndRing}_p$, running in expected time $\mathsf{poly}(\log(p))/\varepsilon_{\mathcal{B}}$,*

$$t = 96s/\varepsilon_{\mathcal{B}} \quad \textit{and} \quad \mathsf{Adv}^{\mathsf{hint\text{-}EndRing}_p}(\mathcal{E},t) \geq 1/4.$$

See the full version of this paper [2] for the proof. Assuming t-$\mathsf{hint\text{-}EndRing}_p$ is a hard problem for quantum algorithms, this is a meaningful result. By using the classical forger, the quantum reduction can efficiently recover a basis for $\mathrm{End}(E)$.

5.5 Expected Hardness of the q-$\mathsf{hint\text{-}EndRing}_p$ Problem

In Theorem 4 and Theorem 6, we proved that SQIsign is EUF-CMA-secure assuming the hardness of q-$\mathsf{hint\text{-}EndRing}_p$(Problem 5) and q-hint-dist (Problem 3). We also discussed the hardness of q-hint-dist in Remark 5.1. Here, we focus on why we do not expect the hints to make $\mathsf{EndRing}_p$easier.

Consider what the $\mathcal{H}_E^{\mathsf{unif}}$ hint distribution does: it samples a degree d according to a weighted distribution, and then it samples a random isogeny (if we consider the composition $\psi_2 \circ \psi_1$) of degree depending on d. In the full version of this paper [2], we show how to sample from a distribution that is negligibly close to the distribution of d, *in polynomial time*. Hence, the only non-trivial information that such a hint provides to the simulator is the isogeny $\psi_2 \circ \psi_1$ itself.

To sample an isogeny according to $\mathcal{H}_E^{\mathsf{unif}}$, the simulator could try the following:

- Factorize[5] the degree of $\psi_2 \circ \psi_1$ as $\deg\psi_2 \circ \psi_1 = \prod_i^t p_i^{e_i}$, and assume that p_t is the largest prime diving $\deg\psi_2 \circ \psi_1$. The complexity of the factorization is polynomial in p_t.
- For every prime p_i:
  - Sample a random point K of $E[p_i]$, which is defined over an extension field of order $O(p_i)$. The complexity is polynomial in p_i.
  - Compute an isogeny with kernel $\langle K \rangle$ with VéluSqrt formulas [9]. The complexity is similarly polynomial in p_i.

[5] It is possible to sample the degree d together with its factorization [5], but it is still necessary to factor the degree of ψ_2.

  - This yields an isogeny of degree p_i. Repeating the process e_i times and concatenating the outputs, produces an isogeny of degree $p_i^{e_i}$.
- Finally, iterating over all t possible p_i and concatenating the outputs gives an uniformly random isogeny of the desired degree.

The complexity of the sampling procedure is polynomial in p_t. Hence, if the degree of $\psi_2 \circ \psi_1$ is sufficiently smooth (i.e., the smoothness bound p_t is in $O(\mathsf{poly}(\lambda))$), the hint does not provide any additional information. Unfortunately, that happens with negligible probability.

In conclusion, the only information the hints provide is the efficient representation of some isogenies of non-smooth degree. Informally, we do not expect these to provide any help in solving the $\mathsf{EndRing}_p$ problem: non-smooth degree isogenies do not provide any extra information compared to smooth-degree isogenies.

6 Discussion and Future Work

In this work, we provided a full proof of security of SQIsign: we gave a reduction of the EUF-CMA security of SQIsign in the ROM to the hardness of two non-interactive problems, the endomorphism ring problem with hints and the hint indistinguishability problem. Through our Fiat–Shamir with hints framework, we expect the same proof techniques to be applicable to all HD variants of SQIsign.

Remaining gaps and limitations. The implementation of SQIsign, in its round-2 submission to the NIST standardization process, differs slightly from the protocol analyzed so far: for efficiency reasons, the implementation relies on some algorithms that could fail. These failure cases can be split into two categories: those that fail with negligible probability and therefore do not affect security, and those that fail with small but not negligible probability (approximately 2^{-64}, according to [1]). This second category has a more significant impact on security: while they are unlikely to be practically exploitable, they introduce a bias in the public keys and signatures that is not captured by our security analysis.

Furthermore, our result in Theorem 6 has a loss factor that is quadratic in the number of signing queries, which is then divided by $\sqrt{p}$. This implies that, for adversaries that make exponentially many signing queries (say, 2^{64} queries against a prime $p \approx 2^{256}$, for NIST security level I), the reduction becomes vacuous.

Takeaways and recommendations. In light of this discussion, we invite the research community to further investigate the algorithmic building blocks of SQIsign that currently have non-negligible failure probability. We expect that developing better algorithms that maintain the same efficiency while obtaining negligible failure probability is within reach. This would close the remaining gap between the theoretical analysis and the implemented version of SQIsign.

Similarly, we suggest that future revisions of SQIsign bring the commitment min-entropy to within $1/p$, rather than $1/\sqrt{p}$. This could be easily achieved at almost no cost by increasing N_{mix} to $\approx 2^{8\lambda}$, but possibly even more efficient solutions exist. With a factor $1/p$, Theorem 6 would be meaningful even in the presence of attackers making exponentially many queries. For example, with 2^{64} queries at NIST security level I, the loss would be roughly 2^{-128}.

Future work. Lastly, we leave the analysis of additional security properties for future work. This includes studying strong unforgeability (which, in its current formulation, SQIsign is unlikely to achieve), the three BUFF properties [12], and a security proof in the quantum random oracle model. The current techniques for a QROM reduction do not seem to apply, so more research is needed.

Acknowledgments. We thank the whole SQIsign team for their help and support throughout this project. This work was funded by ERC grant No. 101116169 (AGATHA CRYPTY); France 2030 program, grants No. ANR-22-PETQ-0008 (PQ-TLS) and ANR-22-PNCQ-0002 (HQI); Danish Independent Research Council, grant No. 1026-00350B (RENAIS); Swiss SNF Consolidator Grant No. 213766 (CryptonIs).

References

1. Aardal, M.A., et al.: SQIsign - Version 2.0. Technical report, National Institute of Standards and Technology (2025). https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures
2. Aardal, M.A., Basso, A., De Feo, L., Patranabis, S., Wesolowski, B.: A complete security proof of SQIsign. Cryptology ePrint Archive, Paper 2025/379 (2025). https://eprint.iacr.org/2025/379
3. Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 418–433. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_28
4. Attema, T., Cramer, R., Kohl, L.: A compressed Σ-protocol theory for lattices. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part II. LNCS, vol. 12826, pp. 549–579. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84245-1_19
5. Bach, E.: How to generate factored random numbers. SIAM J. Comput. **17**(2), 179–193 (1988). https://doi.org/10.1137/0217012
6. Backendal, M., Bellare, M., Sorrell, J., Sun, J.: The Fiat-Shamir zoo: relating the security of different signature variants. In: Gruschka, N. (ed.) NordSec 2018. LNCS, vol. 11252, pp. 154–170. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03638-6_10
7. Basso, A., et al.: Supersingular curves you can trust. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part II. LNCS, vol. 14005, pp. 405–437. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30617-4_14
8. Basso, A., et al.: SQIsign2D-west - the fast, the small, and the safer. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 339–370. Springer, Singapore (2024). https://doi.org/10.1007/978-981-96-0891-1_11

9. Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. Open Book Ser. **4**(1), 39–55 (2020). https://doi.org/10.2140/obs.2020.4.39
10. Borin, G., Lai, Y.F., Leroux, A.: Erebor and Durian: full anonymous ring signatures from quaternions and isogenies. IACR Commun. Cryptol. **1**(4) (2025). https://doi.org/10.62056/ava3zivrzn
11. Chavez-Saab, J., et al.: SQIsign. Technical report, National Institute of Standards and Technology (2023). https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures
12. Cremers, C., Düzlü, S., Fiedler, R., Fischlin, M., Janson, C.: BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures. In: 2021 IEEE Symposium on Security and Privacy, pp. 1696–1714. IEEE Computer Society Press (2021). https://doi.org/10.1109/SP40001.2021.00093
13. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: new dimensions in cryptography. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 3–32. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58716-0_1
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.) ASIACRYPT 2020. LNCS, vol. 12491, pp. 64–93. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64837-4_3
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.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 659–690. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_23
16. Duparc, M., Fouotsa, T.B.: SQIPrime: a dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 396–429. Springer, Singapore (2024). https://doi.org/10.1007/978-981-96-0891-1_13
17. 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.) EUROCRYPT 2018. LNCS, vol. 10822, pp. 329–368. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_11
18. Eisenträger, K., Hallgren, S., Leonardi, C., Morrison, T., Park, J.: Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. Open Book Ser. **4**(1), 215–232 (2020). https://doi.org/10.2140/obs.2020.4.215
19. Kani, E.: The number of curves of genus two with elliptic differentials. Journal für die reine und angewandte Mathematik **1997**(485), 93–122 (1997)
20. Leroux, A.: Quaternion algebras and isogeny-based cryptography. (Algèbres de quaternions et cryptographie à base d'isogénies). Ph.D. thesis, Polytechnic Institute of Paris, France (2022)
21. Nakagawa, K., et al.: SQIsign2D-east: a new signature scheme using 2-dimensional isogenies. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part III. LNCS, vol. 15486, pp. 272–303. Springer, Singapore (2024). https://doi.org/10.1007/978-981-96-0891-1_9
22. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part VI. LNCS, vol. 14656, pp. 388–417. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58751-1_14

23. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_33
24. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Report 2022/1068 (2022). https://eprint.iacr.org/2022/1068
25. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). https://doi.org/10.1109/SFCS.1994.365700
26. Silverman, J.H.: The Arithmetic of Elliptic curves, Graduate Texts in Mathematics, vol. 106. Springer (1986)
27. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 62nd FOCS, pp. 1100–1111. IEEE Computer Society Press (2022). https://doi.org/10.1109/FOCS52979.2021.00109