

Dimension-4 SQIsign at Round-3 Parameters: Sizes and Costs of the Compact Format

Dustin Ray, Anchorage Digital

September 2026

Abstract

SQIsign holds the smallest known combination among post-quantum signatures, and its dimension-2 signature carries an auxiliary curve whose only role is to make the response computable in dimension 2. SQIsignHD’s dimension-4 response has no such curve. We take that construction to the round-3 SQIsign primes, which replaced the round-2 primes in September 2026 after the attacks of Wesolowski and others, on our Rust port of the SQIsign reference code, and measure it in one session next to the reference’s own assembly build. At NIST level I the dimension-4 signature is 142 bytes against 200 for the specification’s format, with an 84-byte public key: 226 bytes for key and signature together, the smallest level-I combination we are aware of, among isogeny schemes and post-quantum signatures alike, at parameters that stand after those attacks. The price is verification: the dimension-4 verifier costs 9.9 times the dimension-2 verifier of the same code (120.3 against 12.2 megacycles). The dimension-4 parameters published with SQIsignHD are for its authors’ own primes; we derive them for the round-3 primes, state which choices are SQIsignHD’s and which are ours, and report what was built and measured.

1 Introduction

SQIsign is a signature scheme whose public key is an elliptic curve and whose signature describes a path of curves. Its first version signed in seconds and verified fast, with the smallest signatures of any post-quantum proposal, at the price of a signer built on the KLPT algorithm for finding paths in the quaternion algebra of the curve [FKL⁺20].

In 2022 three groups broke the SIDH key exchange by showing how an isogeny between two elliptic curves can be recovered from its action on a few points, by embedding it in an isogeny of a higher-dimensional abelian variety [CD23, MMP⁺23, Rob23]. The embedding is Kani’s [Kan97]. What was a weapon against SIDH became a tool for SQIsign: the signer no longer needs a path of smooth degree, because any isogeny of known degree can be handed to the verifier through its action on points and rebuilt in a higher dimension.

SQIsignHD did this in dimension 4 [DLRW24]. Its signer is fast and its signature is small, and the whole cost moved to the verifier, which computes a chain of dimension-4 isogenies. Its authors released a C signer and a SageMath verifier [DLRW25]. SQIsign2D-West brought the response back to dimension 2 [BDF⁺24]: one more isogeny, the auxiliary one, is computed by the signer so that the verifier’s chain runs on a product of two elliptic curves. Verification became fast again, the signature grew by the auxiliary curve, and this design is the round-2 and the round-3 SQIsign submission to NIST [AAA⁺25, AAA⁺26].

In 2026 Wesolowski gave an algorithm for the supersingular isogeny problem in time and memory $p^{1/3+o(1)}$ [Wes26]. The round-3 submission of September 2026 answered with larger primes, $3 \cdot 2^{324} - 1$, $27 \cdot 2^{500} - 1$ and $17 \cdot 2^{664} - 1$ at levels I, III and V [AAA⁺26].

This paper takes SQIsignHD’s dimension-4 response to those primes. We already had a Rust implementation of SQIsign, `squisign-rs`, with the round-3 dimension-2 signer and verifier reproducing the reference’s known-answer vectors byte for byte [Ray26c], and a dimension-4 format of the same crate at the round-2 primes. We derived the dimension-4 parameters for the round-3 primes, built the signer and verifier at level I behind a feature flag, checked the signatures against the SQIsignHD authors’ own verifier re-parameterised to our prime, and measured everything in one session against the reference’s assembly build. Section 2 is a glossary. Section 3 says what exists. Section 4 explains the format and its parameters. Section 5 has the numbers. Section 6 says what none of this changes about strong unforgeability and names the construction that does. Section 7 lists what is missing.

2 Terminology

auxiliary isogeny

In dimension 2, a second isogeny the signer computes next to the response so that the two together fill a $(2^f, 2^f)$ -isogeny the verifier can run. Its target, the auxiliary curve, is sent in the signature. Dimension 4 has none.

challenge

The isogeny the verifier’s hash of the message and the commitment picks from the public key curve; the signer must connect its target to the commitment.

commitment

A fresh random curve the signer publishes first, so that the challenge cannot be chosen after the response.

degree

The size of an isogeny’s kernel; the number of points that map to zero. A degree- q isogeny is “a path of length q ”.

dimension (of the embedding)

The number of elliptic curves whose product carries the verifier’s chain: two in SQIsign2D and the round-3 submission, four in SQIsignHD and here. Each step in dimension g acts on 2^g coordinates.

endomorphism ring

All isogenies from a curve to itself. Knowing it is the secret; the security of every scheme here rests on it being hard to compute for a random supersingular curve.

isogeny

A map between elliptic curves that respects their group law. It is determined by its kernel; “walking” from one curve to another means composing isogenies of small degree.

Kani embedding

Kani’s lemma: an isogeny of degree q between elliptic curves, together with one of degree $N - q$, sits inside an isogeny of degree N between products of curves. In dimension 4 the second isogeny is replaced by a sum of two squares $N - q = a_1^2 + a_2^2$ on the same curves, so nothing extra has to be computed or sent.

KAT

Known-answer test: the reference’s published keys and signatures for fixed seeds, which an implementation must reproduce byte for byte.

megacycle

One million processor cycles, read with `rdtsc`; the unit the reference’s own benchmark reports and the unit of every cost in this paper.

response

The isogeny from the commitment curve to the challenge curve that the signer, and only the signer, can compute. In dimension 4 it is described by its degree q and its action on a few points.

supersingular curve

An elliptic curve over $\mathbb{F}_{p^2}$ whose endomorphism ring is a maximal order in a quaternion algebra. All curves in this paper are supersingular.

theta model

The coordinate system the verifier’s chain runs in. A point of a dimension- g variety has 2^g theta coordinates: four in dimension 2, sixteen in dimension 4.

torsion

The points of a curve whose order divides a given number. The 2^r -torsion is where the response’s action is written down; 2^r divides $p + 1$ on these primes, so those points are defined over $\mathbb{F}_{p^2}$.

3 Related work

SQIsignHD The construction is Dartois, Leroux, Robert and Wesolowski’s [DLRW24]: the response of degree $q < 2^e$ is chosen so that $2^e - q$ is a prime congruent to 1 modulo 4, and the verifier rebuilds it as a $(2^e, 2^e, 2^e, 2^e)$ -isogeny on $E_{\text{com}}^2 \times E_{\text{chl}}^2$ computed as two half-chains that meet in the middle (their Section 4). Their library, version 2.0, has two parts: a C signer that its README describes as a light modification of the SQIsign2D-West implementation, and a SageMath verifier built on the `Theta_dim4` package [DLRW25, Dar25]. It is instantiated on the round-2 SQIsign primes $5 \cdot 2^{248} - 1$, $65 \cdot 2^{376} - 1$ and $27 \cdot 2^{500} - 1$, with $e = \lambda + \lceil \log_2 2\lambda \rceil = 136/201/265$ and $r = \lceil e/2 \rceil + 2 = 70/103/135$ from the parameter script of their library [DLRW25]. The dimension-4 arithmetic itself, 2-isogeny chains in the theta model of level 2 in dimension 4, is Dartois’s [Dar24].

The submissions The round-2 and round-3 SQIsign submissions are dimension-2 schemes in the SQIsign2D-West design [BDF⁺24, AAA⁺25, AAA⁺26]; their reference code is the-sqisign [The25, The26], with a portable and an assembly-backed field arithmetic. The round-3 specification’s Chapter 5 fixes the parameters measured here as the dimension-2 baseline.

sqisign-rs Our crate implements SQIsign round 3 in Rust with the specification’s format, a compressed format of its own that drops one matrix entry and recovers it from two Weil pairings, and the dimension-4 compact format of this paper at level I [Ray26c]. Its round-2 predecessor, tag `v0.4.31`, had the same three formats at the round-2 primes, the compact one at 108 bytes; it is the round-2 code measured in Section 5.

What we did not find To our knowledge the code measured here is the only implementation with a dimension-4 SQIsign signer and verifier in one codebase, at either parameter set. The SQIsignHD authors’ release is a C signer and a SageMath verifier for their primes. A GitHub search on 2026-09-26 for “SQIsignHD”, “SQISignHD” and “Theta_dim4” returned their two repositories and nothing else; we did not search further, and a dimension-4 SQIsign implementation we have missed would change this paragraph and nothing else in the paper.

4 Dimension 4

The cost first The verifier of the compact format runs a chain of dimension-4 isogeny steps, each on sixteen theta coordinates instead of the four of a dimension-2 step, and it runs 87 steps from each end at level I. Measured in Section 5, it costs 9.9 times the dimension-2 verifier of the same crate at the same prime (120.3 against 12.2 megacycles), and 10.6 times the reference’s assembly build.

Why pay it In dimension 2 the response σ of degree q cannot be run by the verifier alone: Kani’s embedding needs a second isogeny of degree $2^f - q$ from the challenge curve, the auxiliary isogeny τ , and the signer computes it and sends its target curve E_{aux} (Figure 1, left). In dimension 4 the second isogeny is replaced by two integers with $a_1^2 + a_2^2 = 2^e - q$, which exist when $2^e - q$ is a prime congruent to 1 modulo 4 and which the verifier finds by Cornacchia’s algorithm from q alone. The chain runs on $E_{\text{com}}^2 \times E_{\text{chl}}^2$ and no other curve is involved (Figure 1, right). Dimension 4 removes the auxiliary curve from the signature, not the auxiliary freedom: another pair (a'_1, a'_2) with the same sum of squares, or another isogeny of degree q from the same curve, still yields a valid signature. What the signature must carry is the commitment curve, the degree q , and the action of σ on a basis of the 2^r -torsion: a 2×2 matrix of scalars modulo 2^r , of which three are sent and the fourth follows from the Weil pairing, $ad - bc \equiv kq \pmod{2^r}$ with k fixed by the two bases [DLRW24, Section 6.1]. At level I that is $2 \cdot 41 = 82$ bytes of curve, 22 bytes of q , three scalars of 12 bytes and two one-byte basis hints: 142 bytes, against 200 for the specification’s format, which carries the auxiliary curve and a matrix modulo 2^{198} . The challenge is not sent: the verifier recomputes it from the public key, the commitment curve and the message, as the round-3 challenge hash does.

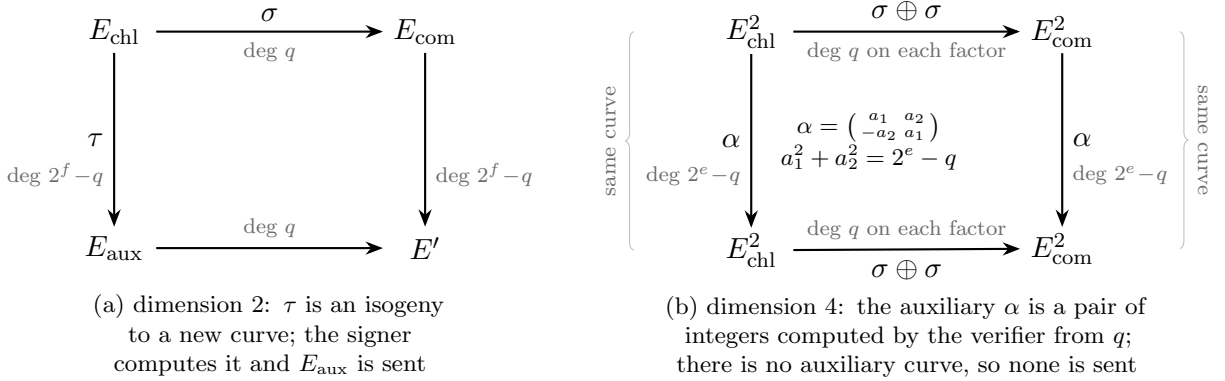


Figure 1: The two ways a verifier rebuilds the response; both are Kani squares. (a) In dimension 2 the response σ of degree q is completed by an auxiliary isogeny τ of degree $2^f - q$ to a new curve; the signer computes τ and the signature carries E_{aux} . (b) In dimension 4 the same square sits on the doubled curves and the complement is the endomorphism $\alpha = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$ with $a_1^2 + a_2^2 = 2^e - q$, which the verifier computes from q ; it acts on E_{chl}^2 and on E_{com}^2 alike, so each column of the square is one curve and there is no auxiliary curve to send. The signature carries E_{com} , q and the action of σ on the 2^r -torsion.

Moving the parameters to round 3 SQIsignHD’s exponent e bounds the response degree, $q < 2^e$. Every ideal class contains an ideal of norm at most about $0.90\sqrt{p}$ [DLRW24, Lemma 12], so 2^e must exceed $\sqrt{p}$, and the paper takes “a few bits over $\sqrt{p}$ ” as sufficient on a heuristic (their Section 4.2). The library’s rule $e = \lambda + \lceil \log_2 2\lambda \rceil$ is written in the security parameter because at the

round-2 primes $p \approx 2^{2\lambda}$; there it is $\log_2 \sqrt{p}$ plus 10.8/10.0/12.6 bits. At the round-3 level I prime, which has 70 bits more than $2^{2\lambda}$, the same formula gives $e = 136$, below the $2^{162.6}$ that Lemma 12 makes the smallest norm any class is sure to contain, so no response would exist. What transfers is the content of the rule, $\sqrt{p}$ plus about ten bits.

We take $e = \lceil (\log_2 p)/2 \rceil + 11 = 174/264/346$ and, by the library’s own rule for the torsion the two half-chains need, $r = \lceil e/2 \rceil + 2 = 89/134/175$ (Table 1). The margin of 11 bits is the library’s at the round-2 primes, where its signer found a good q on every signature; the paper’s own prime uses 15.3. Two checks pin it from below. The number of ideal vectors of norm below 2^e grows as $2^{2 \cdot \text{margin}}$, about 2^{22} candidates against one good norm in a few hundred, so a good q exists with overwhelming probability. And Nakagawa and Onuki’s conservative countermeasure for PRISM-id, whose response reveals an isogeny of large prime degree, is a degree of at least $4\lambda/3$ bits [NO25, Section 5.3]; transferred to e , that is 170.7/256.0/341.3 against 174/264/346, cleared at every level, where 8 bits of margin would not clear it at level I.

The degree The signer samples vectors of the response ideal below 2^e and keeps the first whose norm q is odd, congruent to 3 modulo 4, and has $2^e - q$ a probable prime (40 Miller–Rabin rounds). The verifier repeats the test on q and decomposes $2^e - q$ by Cornacchia. The sampled norms are odd, so one candidate in two passes the congruence; for $2^e - q$ behaving as a random e -bit integer the density of good q is then $1/(e \ln 2)$, one candidate in 121 at level I, and 60 candidates per signature reach a primality test. Section 5 measures the loop.

What the verifier checks The verifier decodes the key and the signature, recomputes the challenge from the public key, the commitment curve and the message, completes the fourth scalar from the pairing relation, tests q for goodness, writes $2^e - q = a_1^2 + a_2^2$ by Cornacchia, and builds the kernel of the dimension-4 isogeny on $E_{\text{com}}^2 \times E_{\text{chl}}^2$ from a_1, a_2 and the transmitted action [DLRW24, Lemma 4 and Section 4.4]. It then computes the two half-chains of $\lceil e/2 \rceil$ steps from both ends and accepts when the two middle codomains agree and the image of a point through the chain is what the transmitted action says, the two conditions of SQIsignHD’s Section 4.5. A signature fails on any decoding error, on a degree that is not good, on a chain that lands on a product of curves where it should not, or on either condition.

Whose choices SQIsignHD’s: the response as an ideal of good norm, the goodness test, the half-chains of $\lceil e/2 \rceil$ steps from both ends with $r = \lceil e/2 \rceil + 2$, the transmitted action modulo 2^r with the fourth scalar from the pairing, the verifier’s two acceptance conditions (the middle codomains agree and the image check of their Section 4.5), and the basis-from-hint convention of their library, kept so that their verifier can check our signatures unmodified. Ours: the primes, e and its margin, the round-3 commitment and its 2^λ challenge with the challenge recomputed rather than sent, the wire format with two hint bytes in place of the library’s packed bits, and the signer’s sampler, which draws lattice vectors of the response ideal and rejects on goodness.

Table 1: Dimension-4 parameters at the round-3 primes. Level I is built and measured; levels III and V are derived only.

	NIST I	NIST III	NIST V
p^a	$3 \cdot 2^{324} - 1$	$27 \cdot 2^{500} - 1$	$17 \cdot 2^{664} - 1$
$\log_2 p^a$	325.58	504.75	668.09
λ , challenge bits ^a	128	192	256
e , response bound $q < 2^{eb}$	174	264	346
$r = \lceil e/2 \rceil + 2$, transmitted torsion bits ^c	89	134	175
half-chain steps $\lceil e/2 \rceil^c$	87	132	173
public key, bytes, predicted ^d	84	130	170
signature, bytes, predicted ^d	142	214	280
public key, bytes, measured	84	not built	not built
signature, bytes, measured	142	not built	not built
round-3 standard signature, bytes ^a	200	306	406

^a The SQIsign round-3 specification [AAA⁺26].

^b Ours: $e = \lceil (\log_2 p)/2 \rceil + 11$ (Section 4).

^c SQIsignHD’s rule for the torsion the half-chains need [DLRW24, Section 4.3].

^d Field-by-field sums of the wire format (Section 4).

5 Benchmarks

Method One session on one machine, Intel Xeon CPU @ 2.80GHz (8 vCPUs, 31 GiB) at 2.80 GHz, on 2026-09-26. One binary measures the Rust code of both rounds: the current crate for round 3 and the round-2 crate at tag `v0.4.31` as a dependency, both compiled by the same `rustc` in release mode with fat link-time optimisation and no target-CPU flag. Each operation is timed with `rdtsc` and the wall clock around the call, and the table reports the median over 50 runs for key generation and signing, 200 for verification, and 100 for the compact signer and verifier. The C reference is the-sqisign at tags `nist-v3` and `nist-v2`, each built with CMake in `Release` mode and `-DSQISIGN_BUILD_TYPE=broadwell`, the assembly-backed field arithmetic, and measured by its own benchmark (`--iterations=300` at level I, 100 at III and V), medians. The round-3 Rust code chooses its assembly field kernels at run time from CPUID; the round-2 crate has no assembly kernels and signs on a big-integer library. Verification is measured from bytes: decode the key, decode the signature, verify.

Sizes Table 2 lists what the session observed on the wire. At level I the compact key and signature together are 226 bytes against 283 for the specification’s format, a saving of 29% on the signature; the compressed dimension-2 format sits between them at 176 bytes. On the round-2 primes the same three formats were smaller by the width of the field.

Table 2: Public key + signature = total, in bytes, as observed in the session. Compact formats are level I only.

primes	format	NIST I	NIST III	NIST V
round 3	standard (specification)	$83 + 200 = 283$	$129 + 306 = 435$	$169 + 406 = 575$
	compressed (this crate)	$83 + 176 = 259$	$129 + 269 = 398$	$169 + 353 = 522$
	compact, dim. 4 (this crate)	$84 + 142 = 226$	not built	not built
round 2	standard (specification)	$65 + 148 = 213$	$97 + 224 = 321$	$129 + 292 = 421$
	compact, dim. 4 (crate v0.4.31)	$64 + 108 = 172$	not built	not built

Cycles Table 3 is the session in megacycles. The dimension-4 verifier costs 9.9 times the dimension-2 verifier of the same crate at level I; on the round-2 primes the same crate’s dimension-4 verifier cost 8.0 times its dimension-2 one. Signing in dimension 4 costs 3.0 times the dimension-2 signer: the good degree is found by rejection, and the loop is measured in Table 5. Key generation is the round-3 key generation in both formats and differs only in the basis convention (41.7 against 39.0 megacycles). The round-3 dimension-2 verifier of the crate runs at 1.08 times the reference’s assembly build at level I, its key generation at 1.10 times and its signing at 1.12 times; the compressed format’s recovery adds 18 % to a verification.

The round-2 rows The lower half of Table 3 is the same two designs on the round-2 primes, measured in the same session. The reference’s assembly build verifies a round-2 signature in 5.3 megacycles and a round-3 one in 11.3: the price of the primes moved by the 2026 attack, at the same design. The round-2 crate’s dimension-4 verifier cost 8.0 times its dimension-2 verifier; on the round-3 prime the multiple is 9.9, with half-chains of 87 steps instead of 68 on a field of six 64-bit limbs instead of four. The round-2 crate has no assembly field kernels and signs on a big-integer library, and its rows say so.

Table 3: Megacycles, medians of the session. The last column is the dimension-4 verifier over the dimension-2 verifier of the same code and primes. The C reference is the **broadwell** build.

implementation	level	keygen	sign	verify	× dim. 2
<i>round-3 primes</i>					
C reference, dimension 2	I	35.5	101.4	11.3	
C reference, dimension 2	III	111.4	371.0	28.7	
C reference, dimension 2	V	241.5	780.6	79.8	
Rust, dimension 2	I	39.0	113.5	12.2	
Rust, dimension 2	III	137.8	448.1	32.7	
Rust, dimension 2	V	280.1	922.6	83.0	
Rust, dimension 2, compressed verify	I			14.4	
Rust, dimension 4 (compact)	I	41.7	336.6	120.3	9.9
<i>round-2 primes</i>					
C reference, dimension 2	I	48.4	112.4	5.3	
C reference, dimension 2	III	136.9	314.4	17.0	
C reference, dimension 2	V	210.6	527.4	32.6	
Rust, dimension 2	I	175.8	429.3	13.6	
Rust, dimension 2	III	412.2	1653.7	38.2	
Rust, dimension 2	V	1169.8	3036.1	77.1	
Rust, dimension 4 (compact)	I	173.8	204.6	108.6	8.0

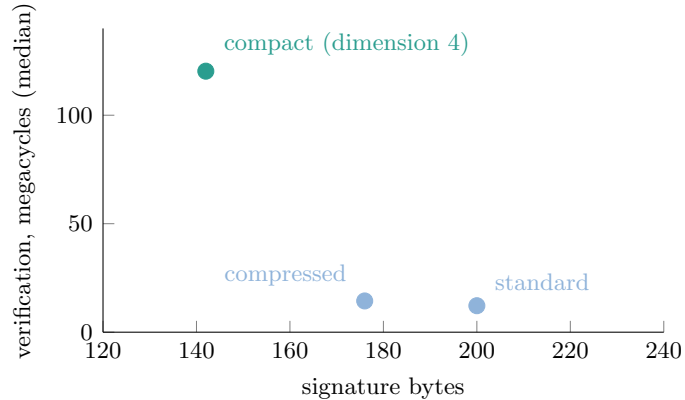


Figure 2: The trade at level I on the round-3 prime: signature bytes against verification cost for the three formats of one crate, from the session of Table 3.

Milliseconds Table 4 gives wall-clock times on two machines for level I. Neither machine is what a deployment runs; the ratio between the rows is the number to carry, and it is the same on both.

Table 4: Wall-clock milliseconds at level I, medians. The M4 Pro column is pending the author’s run on that machine.

format	operation	Xeon, 2.80 GHz (ms)	M4 Pro (ms)
round 3, dimension 2 (standard)	key generation	13.9	pending
	signing	40.5	pending
	verification	4.4	pending
	verification, compressed	5.1	pending
round 3, dimension 4 (compact)	key generation	14.9	pending
	signing	120.2	pending
	verification	43.0	pending
round 2, dimension 2 (standard)	key generation	62.8	pending
	signing	153.3	pending
	verification	4.8	pending
round 2, dimension 4 (compact)	key generation	62.1	pending
	signing	73.1	pending
	verification	38.8	pending

The rejection loop Table 5 counts the compact signer’s search for a good degree over the session’s signatures against the expectation of Section 4. A candidate costs one norm; one in two reaches a Miller–Rabin test on an e -bit number, and composites fail at the first round. The spread of signing times in the table is this loop: the median signature needs 68 samples, the mean 114, and the session saw 1 to 835.

Table 5: The compact signer’s good-degree loop at level I: measured over the session’s signatures against the density $1/(e \ln 2)$ for odd q (and the figure for a candidate of random parity, which the sampler does not produce).

	measured	expected
signatures measured	100	
response samples per signature, mean	114	121
the same if q had random parity		241
response samples per signature, median (min, max)	68 (1, 835)	
primality tests per signature, mean	57	60
signing, Mcycles, median (min, max)	337 (50, 3712)	
signing, dimension 2, Mcycles, median	114	

Memory One compact verification at level I allocates 1674 KiB of heap at its peak (1.64 MiB), measured with a counting allocator around the call; the dimension-2 verifier allocates nothing.

6 Strong unforgeability, briefly, and ECLIPSE

A signature scheme is strongly unforgeable when no one can produce a second valid signature on a message already signed. The SQIsign family is not: in the dimension-2 format the auxiliary isogeny can be replaced by another of the same degree, giving a second signature that verifies under the same key. The round-3 specification states this in its Section 8.4.2 [AAA⁺26], and the mechanism is written out in [Ray26a]. Dimension 4 removes the auxiliary curve from the wire but not the property: a second isogeny of the same degree from the same commitment curve, with its own action on the torsion, is still a valid second signature. This is a property of the scheme, not a finding of this paper.

A construction that is strongly unforgeable by design exists. The PRISM authors describe, next to their salted scheme, a variant whose signature is one isogeny of prime degree $2^{2e-1} - s^2$ from the public key curve, and state that the EUF-CMA proof of the salted scheme applies to a salted version of it [BBC⁺26, Section 5 and Remark 11]; we call that variant strong-PRISM. Our instantiation of it on the round-3 primes is named ECLIPSE¹ and is the subject of a forthcoming paper.

Dimension 4 buys strong-PRISM nothing. A PRISM signature carries no auxiliary curve in any dimension, so there is nothing for dimension 4 to remove; a dimension-4 instantiation would have the same layout within a few bytes, and its hash target, a prime q with $2^a - q$ prime and congruent to 1 modulo 4, is a second-order prime event, far sparser than the single-prime target of the dimension-2 variant. A feasibility study carried out for prism-rs [Ray26b] measured both and declined the dimension-4 route.

7 Closing notes

Gaps One implementation. There is no independent round-3 dimension-4 signer to compare against; the SQIsignHD authors’ verifier, re-parameterised to our prime and left otherwise unmodified, accepts our signatures and rejects tampered ones, which establishes that it agrees with our verifier on our signer’s output and nothing more [DLRW25]. Levels III and V are derived in Table 1 and

¹ECLIPSE stands for Encoding-Canonical Large-prime Isogeny Signature Extension. The underlying construction, which we call strong-PRISM, is Section 5 of [BBC⁺26] with the salt of Section 6 as suggested in Remark 11; the authors did not name it.

not built. Constant time was not attempted for the dimension-4 signer or verifier; the verifier’s integer arithmetic on the degree is variable-time on public data, and SQIsign signing is variable-time by design in the reference as well. The security argument is SQIsignHD’s with our parameters substituted and has not been re-examined; the existence of a good degree in every class is a heuristic in their paper and stays one here. The format is experimental and not for production.

The field Three years separate the break of SIDH from a two-dimensional SQIsign in a NIST round, and one more separates that from primes moved by a new attack on the isogeny-path problem. Every construction in this paper is young, ours included, and the numbers here describe code as it is in September 2026, not a settled design. That is the reason for caution in using any of it.

Thanks To the SQIsign authors, Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit and Benjamin Wesolowski, and the SQIsign2D-West and round-3 team, for the scheme and the reference code we ported; to the SQIsignHD authors, Pierrick Dartois, Antonin Leroux, Damien Robert and Benjamin Wesolowski, for the dimension-4 construction, its library and the Sage verifier that checks our signatures; and to the PRISM authors, Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren and Benjamin Wesolowski, for the construction that Section 6 names.

References

- [AAA⁺25] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign – algorithm specifications and supporting documentation, version 2.0. NIST PQC Digital Signatures Round 2 Submission, 2025. <https://sqisign.org/spec/sqisign-20250205.pdf>.
- [AAA⁺26] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Giacomo Borin, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Thomas Espitau, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, Riccardo Invernizzi, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Marzio Mula, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, Frederik Vercauteren, Alexandre Wallet, Benjamin Wesolowski, and Wessel van Woerden. SQIsign – algorithm specifications and supporting documentation, version 3.0. NIST PQC Digital Signatures Round 3 Submission, 2026. <https://sqisign.org/spec/sqisign-20260901.pdf>.
- [BBC⁺26] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM with a pinch of salt: Simple, efficient and strongly unforgeable signatures from isogenies. Cryptology ePrint Archive, Paper 2026/443, 2026. Published

- in the *Journal of Cryptology* 39(4), article 30, 2026, doi 10.1007/s00145-026-09585-6. <https://eprint.iacr.org/2026/443>.
- [BDF⁺24] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-West: The fast, the small, and the safer. In *Advances in Cryptology – ASIACRYPT 2024*, volume 15486 of *LNCS*, pages 339–370. Springer, 2024. ePrint 2024/760.
 - [CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, volume 14008 of *LNCS*, pages 423–447. Springer, 2023.
 - [Dar24] Pierrick Dartois. Fast computation of 2-isogenies in dimension 4 and cryptographic applications. Cryptology ePrint Archive, Paper 2024/1180, 2024. <https://eprint.iacr.org/2024/1180>.
 - [Dar25] Pierrick Dartois. Theta_dim4: SageMath library for 2-isogenies in dimension 4 in the theta model. https://github.com/Pierrick-Dartois/Theta_dim4, 2025.
 - [DLRW24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New dimensions in cryptography. In *Advances in Cryptology – EUROCRYPT 2024*, volume 14651 of *LNCS*, pages 3–32. Springer, 2024. ePrint 2023/436, revised 2024-09-20; <https://eprint.iacr.org/2023/436>.
 - [DLRW25] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD library, version 2.0: a C signer and a SageMath verifier. <https://github.com/Pierrick-Dartois/SQIsignHD-lib>, 2025. master at commit 0287566.
 - [FKL⁺20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQIsign: Compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology – ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 64–93. Springer, 2020. ePrint 2020/1240.
 - [Kan97] Ernst Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.*, 485:93–122, 1997.
 - [MMP⁺23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, volume 14008 of *LNCS*, pages 448–471. Springer, 2023.
 - [NO25] Kohei Nakagawa and Hiroshi Onuki. Attacks on PRISM-id via torsion over small extension fields. Cryptology ePrint Archive, Paper 2025/1602, 2025. <https://eprint.iacr.org/2025/1602>.
 - [Ray26a] Dustin Ray. Auxiliary isogeny freedom in SQIsign’s two-dimensional representation. Cryptology ePrint Archive, Paper 2026/1305, 2026. Revised 2026-07-08; <https://eprint.iacr.org/2026/1305>.
 - [Ray26b] Dustin Ray. prism-rs: PRISM on the SQIsign round-3 substrate. Software and documentation, <https://github.com/anchorlabsinc/prism-rs>, 2026.

- [Ray26c] Dustin Ray. sqisign-rs: SQIsign round 3 in pure Rust, with the compressed and the dimension-4 compact formats. <https://github.com/anchorageoss/sqisign-rs>, 2026. the code measured is commit 14361c0, the 0.6 merge (workspace version 0.6.0), released as tag v0.6.34 at commit e6ccbc5, its version bump; the round-2 crate measured here is tag v0.4.31, commit a03b834.
- [Rob23] Damien Robert. Breaking SIDH in polynomial time. In *Advances in Cryptology – EUROCRYPT 2023*, volume 14008 of *LNCS*, pages 472–503. Springer, 2023.
- [The25] The SQIsign team. the-sqisign: reference implementation of SQIsign, round 2. <https://github.com/SQISign/the-sqisign>, 2025. tag nist-v2, commit 91e9e46.
- [The26] The SQIsign team. the-sqisign: reference implementation of SQIsign, round 3. <https://github.com/SQISign/the-sqisign>, 2026. tag nist-v3, commit 6d017708.
- [Wes26] Benjamin Wesolowski. The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$. Cryptology ePrint Archive, Paper 2026/1486, 2026. <https://eprint.iacr.org/2026/1486>.