NIST Internal Report
NIST IR 8528

Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Maxime Bros
Pierre Ciadoux
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Hamilton Silberg
Daniel Smith-Tone
Noah Waller

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8528

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8528

Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Maxime Bros
Pierre Ciadoux
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Hamilton Silberg
Daniel Smith-Tone
Noah Waller
Computer Security Division
Information Technology Laboratory

Yi-Kai Liu
Applied and Computational Mathematics Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8528

October 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-10-16

How to cite this NIST Technical Series Publication:
Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Silberg H, Smith-Tone D, Waller N (2024) Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8528. https://doi.org/10.6028/NIST.IR.8528

Author ORCID iDs
Gorjan Alagic: 0000-0002-0107-6037
Maxime Bros: 0000-0001-7838-2529
Pierre Ciadoux: 0009-0001-2272-681X
David Cooper: 0009-0001-2410-5830
Quynh Dang: 0009-0005-9801-6805
Thinh Dang: 0000-0001-9705-0925
John Kelsey: 0000-0002-3427-1744
Jacob Lichtinger: 0000-0003-2407-5309
Yi-Kai Liu: 0000-0001-7458-4721
Carl Miller: 0000-0003-1917-1531
Dustin Moody: 0000-0002-4868-6684
Rene Peralta: 0000-0002-2318-7563
Ray Perlner: 0000-0001-8793-2238
Angela Robinson: 0000-0002-1209-0379
Hamilton Silberg: 0009-0004-4178-8954
Daniel Smith-Tone: 0000-0002-7995-8734
Noah Waller: 0000-0002-6979-9725

Contact Information
pqc-comments@nist.gov

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8528/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

NIST is in the process of evaluating public-key digital signature algorithms for potential standardization to protect sensitive information into the foreseeable future, including after the advent of quantum computers. Any signature scheme that is eventually selected would augment FIPS 204, Module-Lattice-Based Digital Signature Standard; FIPS 205, Stateless Hash-Based Digital Signature Standard; FIPS 186-5, Digital Signature Standard (DSS); and SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes. This report describes the evaluation criteria and selection process of the First Round of the Additional Digital Signatures for the NIST Post-Quantum Cryptography (PQC) Standardization Process. Based on public feedback and internal reviews of the first-round candidates, NIST selected 14 candidate algorithms to move forward to the second round of evaluation: CROSS, FAEST, HAWK, LESS, MAYO, Mirath (merger of MIRA/MiRitH), MQOM, PERK, QR-UOV, RYDE, SDitH, SNOVA, SQIsign, and UOV.

Keywords

cryptography; digital signatures; post-quantum cryptography; quantum-resistant; quantum safe.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Contents

List of Tables

Supplemental Content

The NIST Additional Digital Signatures for PQC Standardization Process webpage is available at https://csrc.nist.gov/Projects/pqc-dig-sig/standardization.

Acknowledgments

NIST would like to thank all of the candidate submission teams who developed, designed, and analyzed the post-quantum public-key digital signature algorithms and prepared detailed submission packages.

NIST is also grateful for the efforts of those in the cryptographic community who provided security, implementation, and performance analyses of the candidate algorithms during the first round. NIST would not be able to select additional post-quantum digital signature algorithms for standardization without the combined efforts of these individuals and the algorithm submitters.

The authors of this report are also appreciative of the efforts by other members of NIST's PQC team who reviewed candidate algorithms, analyses, and public comments; performed testing; provided technical and administrative support; and participated in numerous meetings to discuss the selection of the second-round candidates. They are Zuzana Bajcsy, Larry Bassham, Lily Chen, Morris Dworkin, Sara Kerman, and Andrew Regenscheid.

1. Introduction

The National Institute of Standards and Technology (NIST) initiated the public Post-Quantum Cryptography (PQC) Standardization Process in December 2016 to select quantum-resistant public-key cryptographic algorithms for standardization in response to the substantial development and advancement of quantum computing. After three rounds of evaluation and analysis, NIST announced the selection of the first algorithms to be standardized [1]. The public-key encapsulation mechanism (KEM) selected for standardization was CRYSTALS-Kyber (ML-KEM). The digital signatures selected were CRYSTALS-Dilithium (ML-DSA), Falcon (FN-DSA), and SPHINCS$^+$ (SLH-DSA). Except for SPHINCS$^+$, all of these schemes are based on the computational hardness of problems that involve structured lattices. While several non-lattice-based KEMs remained under consideration in the fourth round, no signature schemes remained.

In July 2022, NIST called for additional digital signature proposals to be considered in the PQC standardization process to diversify its post-quantum signature portfolio. Since two signature schemes based on structured lattices had already been standardized, NIST expressed particular interest in additional general-purpose signature schemes based on a security assumption that did not use structured lattices as well as signature schemes with short signatures and fast verification.

NIST published the Call for Proposals for Additional Digital Signatures [2], which specified the submission requirements and evaluation criteria, and received 50 submission packages on June 1, 2023. Of those, NIST accepted 40 First-Round Candidates that consisted of signature schemes based on a variety of different security assumptions. The submission packages of the first-round candidates were posted online at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures for public review and comment.

The Fifth NIST PQC Standardization Conference was held in Rockville, Maryland, on April 10-12, 2024. The submission teams of the accepted first-round candidates were invited to present posters for their candidate algorithms. Throughout the first round, NIST received significant feedback from the cryptographic community. Based on the public feedback and internal reviews of the first-round candidates, NIST announced the selection of 14 signature algorithms as Second-Round Candidates in October 2024 to move forward to the next stage of the standardization process.

Table 1 shows a timeline of major events with respect to the Additional Digital Signatures for the NIST PQC Standardization Process to date.

Table 1. Timeline of the Additional Digital Signatures for the NIST PQC Standardization Process

Date	*Event*
July 2022	NIST announced a forthcoming Call for Proposals for Additional Digital Signatures to diversify its portfolio [1].
September 2022	The Call for Proposals for Additional Digital Signatures was published, outlining the submission requirements and evaluation criteria [2].
June 2023	Submission deadline for the Additional Digital Signatures process.
July 2023	NIST announced 40 First-Round candidates. The public comment period for the first-round candidates began.
April 2024	The Fifth NIST PQC Standardization Conference was held in Rockville, Maryland. Submission teams presented posters for their candidate algorithms.
October 2024	NIST announced 14 Second-Round candidates. NIST IR 8528, *Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process*, was released. The public comment period for the second-round candidates began.

1.1. Purpose and Organization of This Document

The purpose of this document is to report on the first round of the NIST PQC Standardization Process.

Section 2 enumerates the candidates that were included in the first round. It also describes the evaluation criteria and selection process used to ultimately select the second-round candidates.

Section 3 summarizes each of the second-round candidates with a brief description of the algorithm, the properties of interest, and characteristics that might cause some concern. This report focuses on the reasons why candidate algorithms were selected rather than providing detailed justifications for why candidate algorithms were not selected.

Section 4 describes the next steps in the Additional Digital Signatures for the NIST PQC Standardization Process, including provisions for allowable modifications to the second-round candidates and the evaluation process for selecting finalists.

2. Evaluation Criteria and the Selection Process

2.1. Acceptance of the First-Round Candidates

NIST received 50 candidate algorithm submission packages by the entry deadline of June 1, 2023. Of these, NIST accepted 40 first-round candidates that met both the submission requirements and the minimum acceptability criteria for being "complete and proper submissions," as defined in [2].

Table 2. First-round digital signature candidates organized by category, with the candidates selected to advance to the second round bolded and in blue. The starred signature schemes MIRA and MiRitH merged to form a new candidate Mirath.

Code-Based	Lattice-Based	MPC-in-the-Head	Multivariate
CROSS	EagleSign	Biscuit	3WISE
Enhanced pqsigRM	EHTv4	**MIRA***	DME-Sign
FuLeeca	HAETAE	**MiRitH***	HPPC
LESS	**HAWK**	**MQOM**	**MAYO**
MEDS	HuFu	**PERK**	PROV
WAVE	Raccoon	**RYDE**	**QR-UOV**
	SQUIRRELS	**SDitH**	**SNOVA**
Other			TUOV
ALTEQ	Symmetric-Based	Isogeny-Based	**UOV**
eMLE-Sig 2.0	AIMer	**SQIsign**	VOX
KAZ-SIGN	Ascon-Sign		
PREON	**FAEST**		
Xifrat1-Sign.I	SPHINCS-alpha		

The criteria for determining the first round candidates included provisions for reference and optimized C code implementations, known-answer tests, a written specification, and required intellectual property statements. These were the sole criteria used to judge the submission packages. Other factors, such as security, cost, and algorithm and implementation characteristics of the candidates were not considered during the review process prior to the first round, nor did cryptanalysis or performance data of a submission impact the acceptance of the first-round candidates.

2.2. Evaluation Criteria

NIST's Call for Proposals [2] identified three broad aspects of the evaluation criteria that would be used to compare candidate signature algorithms throughout the NIST PQC Standardization Process: 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. As NIST seeks to diversify its signature portfolio, submissions also needed to significantly differ from signature schemes that have already been selected

by NIST for standardization. In particular, the Call for Proposals specifically stated that submissions should, at a minimum, meet one of the following criteria:

- Lattice-based schemes should provide at least one large performance advantage over both CRYSTALS-Dilithium and Falcon.
- Non-lattice-based algorithms should provide at least one large performance advantage over SPHINCS$^+$.

2.3. Security

As with the PQC Standardization Process, security was the most important factor when evaluating the candidate signature algorithms. NIST intends to standardize post-quantum signatures for use in a wide variety of internet protocols (e.g., TLS, SSH, IKE, IPsec, OCSP, and DNSSEC) and other applications (e.g., certificate transparency, document signing, code signing, and firmware updates).

Submitters were encouraged but not required to provide proofs of security in relevant models. Digital signature schemes needed to enable existentially unforgeable signatures with respect to an adaptive chosen message attack (EUF-CMA security).

NIST defined five security categories to compare the security strengths provided by the submissions. Submitters were asked to provide a preliminary classification, according to the definitions provided in [2], with a focus on meeting the requirements for categories 1, 2, and/or 3. It was also recommended that submitters provide at least one parameter set with a substantially higher level of security (i.e., either category 4 or 5).

NIST also listed other desirable security properties, such as resistance to side-channel and multi-key attacks and resistance to misuse. Submissions were encouraged to note additional desirable security properties provided beyond standard unforgeability (e.g., exclusive ownership, message-bound signatures, and non re-signability). Finally, NIST required submission packages to summarize known cryptanalytic attacks on the scheme and complexity estimates for these attacks.

2.4. Cost and Performance

The second-most important criterion when evaluating candidate algorithms involved cost and performance, including:

- The size of public keys and signatures
- Computational efficiency of the signing and verification operations, as well as key generation (i.e., the speed of the algorithms)

Memory requirements refer to both code size and random-access memory (RAM) requirements for software implementations, as well as gate counts for hardware implementations.

The Call for Proposals required all submitters to include performance estimates on the NIST reference platform — an Intel x64 that runs Windows or Linux and supports the GCC compiler. NIST performed a preliminary efficiency analysis on the reference platform but also invited the public to conduct similar tests on additional platforms. NIST hopes that candidate algorithms will offer comparable or improved performance over the currently standardized algorithms.

2.5. Algorithm and Implementation Characteristics

The Additional Digital Signatures for the NIST PQC Standardization Process received many candidate algorithms with new and unique designs and features that are not present in the current NIST standardized public-key algorithms. NIST prefers candidate algorithms with greater flexibility (e.g., those capable of running efficiently on a wide variety of platforms and those that used parallelism or instruction set extensions to achieve higher performance) and simple and elegant designs that reflect the submission team's understanding and confidence. Finally, NIST considered factors that could hinder or promote the adoption of an algorithm or implementation, such as intellectual property or terms of licenses to interested parties.

2.6. Selection of the Candidates to Advance to the Second Round

NIST selected 14 second-round candidates from the 40 first-round candidates using the evaluation criteria specified in [2]. In relative order of importance, NIST considered the security, cost and performance, and algorithm and implementation characteristics of a candidate in selecting the second-round candidates.

NIST evaluated the security arguments presented in the submission packages, internal and external cryptanalysis, and the overall quantity, quality, and maturity of analysis relevant to each candidate, including the analysis of similar schemes. NIST also considered attacks that directly demonstrated that a candidate fell short of NIST's stated security targets as well as attacks that brought the candidate's underlying security assumptions into question or showed room for improvement.

When evaluating the performance of the candidates, NIST considered the public key and signature sizes as well as the computational estimates given in the submission documentation. NIST also established internal performance benchmarks and considered the external feedback and performance estimates that were provided by the cryptographic community.

In a few cases, a submitted design was selected in part for its uniqueness and elegance. NIST generally favored designs that were based on clear design principles or otherwise illustrated an innovative idea. This diversity of designs will enable cryptographers and cryptanalysts to expand the scope of ideas in their field and make it harder for a single type of attack to eliminate the bulk of the candidates remaining in the standardization process.

The algorithms that were not selected to advance to the next round are not under consideration for standardization by NIST.

Table 3. Second-round digital signature candidates organized by category

Code-Based	Lattice-Based	MPC-in-the-Head	Multivariate
CROSS	Hawk	Mirath (MIRA/MiRitH)	UOV
LESS		MQOM	MAYO
		PERK	QR-UOV
Symmetric-Based	Isogeny-Based	RYDE	SNOVA
FAEST	SQIsign	SDitH	

3. Summary of the Second-Round Candidates

This section describes each of the second-round candidates, including their advantages and disadvantages, and why a scheme was selected to advance to the second round.

3.1. CROSS

CROSS [3] is a signature scheme that uses the Fiat-Shamir transform on a zero-knowledge proof of knowledge (ZKPoK) identification protocol. CROSS has two variants, each depending on the NP-hard hardness of one of the two variants of the Syndrome Decoding Problem (SDP): the Restricted Syndrome Decoding Problem (R-SDP) and the Restricted Syndrome Decoding Problem with subgroup G (R-SDP(G)). The security of R-SDP is considered more conservative than that of R-SDP(G). However, schemes based on the R-SDP(G) problem offer better performance in both signature size and algorithm runtime.

CROSS implements both variants with parameter sets at levels 1, 3, and 5. Additionally, each parameter set has a "fast" and "small" version, like SLH-DSA. These fast and small versions have signature sizes similar to the corresponding SLH-DSA parameter sets. Several parameter sets of CROSS — especially the three fast parameter sets under the R-SDP(G) — have noticeably smaller signature sizes than their corresponding SLH-DSA parameter sets. All parameter sets of CROSS have small public keys. CROSS has a similar verification runtime as SLH-DSA but a significantly reduced signature generation time (particularly for the small versions compared to SLH-DSA) and very quick key generation (similar to ML-DSA).

While there are no known attacks against either of the two CROSS variants, the problems are relatively new. NIST looks forward to further analysis of the underlying problems and the ZKPoK identification protocol. CROSS has advanced to the second round in part due to NIST's interest in it as a non-lattice scheme that demonstrates performance benefits over SLH-DSA.

3.2. LESS

LESS [4] is constructed by applying the Fiat-Shamir transform to an interactive ZKPoK of the solution to a computational code equivalence problem. The security of LESS is based on the difficulty of the Linear Equivalence Problem (LEP): recovering the secret isometry that maps a given full-rank generator matrix to the public key (a full-rank generator matrix in systematic form). One round of the protocol results in a soundness error of $\frac{1}{2}$. Soundness error is sufficiently reduced by generating s private isometries that map to multiple public keys for each protocol instance and repeating the protocol t times.

LESS signatures are smaller than SLH-DSA with much larger public keys. Recent work has emerged to use the Canonical Form Linear Equivalence Problem, which results in even smaller signatures (i.e., less than 3Kb) for the same public key sizes [5].

The LEP (and a canonical form version of LEP) will require more analysis to build confidence in the security of LESS. While an updated version of LESS based on the canonical form LEP would offer a non-lattice-based digital signature with signature sizes comparable to ML-DSA, it is unclear how competitive the overall performance profile will be compared to UOV-based signature schemes.

3.3. HAWK

HAWK [6] is a lattice-based hash-and-sign signature scheme that is closely related to Falcon. The central mathematical objects in HAWK are matrices of elements from the same family of rings used in the lattice-based algorithms chosen for standardization. The secret key is an efficient basis for the lattice. To sign, a message is hashed and interpreted as a vector $\mathbf{h}$. The efficient basis is then used to find an element in the lattice that is sufficiently close to $\mathbf{h}$ without leaking information about the secret key. In order to keep the efficient basis secret, Falcon uses the Fast Fourier Transform, which uses floating point arithmetic. In contrast, HAWK, relies on the one more shortest vector problem (omSVP) and search module lattice isomorphism problem (smLIP) to keep secret information from leaking.

NIST has chosen to keep HAWK under consideration because of its strong performance. Due to their similarities, HAWK has a similar performance profile to Falcon. The key and signature sizes for HAWK are comparable — and, in some instances, better — than those of Falcon. Additionally, while Falcon uses floating-point arithmetic, HAWK can be implemented without the use of floating-point arithmetic.

However, the security arguments for HAWK use elements that are not as well-studied as those for Falcon. The authors of HAWK center their security argument on two problems that are variants of more conventional lattice problems: omSVP and smLIP. NIST encourages the community to study the security arguments and underlying assumptions for HAWK more deeply in order to enable further comparison with NIST's current signature standards.

3.4. Mirath (MIRA/MiRitH)

MIRA [7] and MiRitH [8] are signature schemes constructed in the Multi-Party Computation in the Head (MPCitH) paradigm. Signatures for both schemes are generated by applying the Fiat-Shamir transform to a ZKPoK of the solution of the MinRank problem. Security for both MIRA and MiRitH is based on the hardness of the MinRank problem: given k matrices of dimension $m \times n$ over a field $\mathbb{F}_q$, a linear combination with rank r must be found.

MIRA and MiRitH contain variants that use a hypercube structure, which is an optimization within the MPCitH paradigm [9] that uses additive secret sharing, allowing the MPCitH protocol to be parallelized. This optimization also allows for $D+1$ computations rather than 2^D, where D is the number of parallel repetitions of the protocol, requiring higher computational costs while containing smaller signatures.

Both schemes have parameter sets with key sizes in between SLH-DSA and Falcon and signature sizes that are similar to SLH-DSA. The performance for key generation of both schemes is similar to ML-DSA, while the performance for signing and verifying sits between ML-DSA and Falcon. With ongoing research and evolving techniques in the MPCitH paradigm, signature sizes are expected to improve [10], while underlying security assumptions should remain unchanged.

NIST advanced Mirath, a merged submission that combines MIRA and MiRitH [11], to the second round as a result of its competitive performance with other MPCitH schemes.

3.5. MQOM

MQOM [12] is a signature built on the MPCitH paradigm based on the hardness of solving a random multivariate system of quadratic equations with an equal number of variables and equations. While the problem of solving multivariate quadratic systems has been well-studied, the recent result of [13] may have a small effect on the MQOM parameters needed to meet the target security levels.

As with other signatures based on *in the head* techniques, such as MPCitH, Threshold in the Head and Vector Oblivious Linear Evaluation in the Head (VOLEitH), MQOM offers very small public keys with signatures of intermediate size between those of ML-DSA and SLH-DSA. It is expected that significant improvements in the performance and signature size of MQOM will be obtained using new techniques (i.e., techniques from Threshold in the Head) [10] that will not change the underlying security assumptions.

Overall, even if the parameters may need to be adjusted, MQOM is expected to have highly competitive performance within the fast-moving area of MPC/VOLE/Threshold in the Head signatures. NIST hopes that second-round tweaks of MQOM (and the other MPC/VOLE/Threshold in the Head signatures) will yield a better understanding of the possible performance trade-offs and signature sizes that can be obtained from various well-known hardness assumptions.

3.6. PERK

PERK [14] is a signature that consists of a ZKPoK of a secret permutation. Given a matrix $\mathbf{H}$ and an array $\mathbf{x}$, the signatory proves that they know a permutation π such that $\pi(\mathbf{x})$ is in the kernel of H (i.e., $\mathbf{H}(\pi(\mathbf{x})) = \mathbf{0}$). The security assumption, called the Permuted Kernel Problem, is that it is hard to find such a permutation given random $\mathbf{H}$ and $\mathbf{x}$ over a finite field $\mathbb{F}_q$. The proof uses MPC techniques. The computation is simulated by replacing random choices with the result of a hash on the message being signed.

As with other MPCitH schemes, the underlying techniques for building the ZKPoK were vastly improved after the initial submission was received. For PERK in particular, the submitted version relied on a possibly stronger assumption than the Permuted Kernel Problem. An updated version proposed by the PERK team resolves that issue and should achieve a significant reduction in the length of the signature.

Even with these improvements, PERK is expected to be slower than ML-DSA and comparable in speed to SLH-DSA. The size of the PERK signature is expected to be larger than ML-DSA but significantly smaller than SLH-DSA.

The Permuted Kernel Assumption is PERK's only hardness assumption beyond standard assumptions from symmetric-key cryptography. Although the problem was proposed about 30 years ago, there is uncertainty about its concrete complexity. More research on this assumption would help increase confidence in the concrete parameters of PERK for various security levels.

3.7. RYDE

RYDE [15] is a signature scheme constructed in the MPCitH paradigm. Like other MPCitH signature schemes, the construction of RYDE involves generating a random equation together with a solution. The satisfiability of such an equation and the knowledge of a solution as a witness are proved in zero-knowledge. A Fiat-Shamir transform is applied to remove the interaction between the prover and the verifier.

The design of RYDE revolves around the conjecturally hard problem of Rank Syndrome Decoding, which is to solve a system of linear equations over a finite field for a solution of small rank, where rank is defined in a special way for a tuple of elements in a finite extension of a prime field. RYDE uses a slight optimization of the rank-checking protocol in [16]. Given a set of arithmetic constraints that represent an instance of the Rank Syndrome Decoding problem, RYDE produces two variants of the signature scheme by applying two different MPCitH techniques: the hypercube approach using additive secret sharing [17] and Threshold Computation in the Head with linear threshold secret sharing [18, 19]. Significant improvements to RYDE were proposed during round one, including new modelling for the Rank Syndrome Decoding problem and adoption of the VOLEitH framework [20].

NIST advanced RYDE to the second round of evaluation because of the scheme's competitive performance within the category of MPCitH and VOLEitH signature schemes, especially with the recent proposed improvements. The underlying hard problem of Rank Syndrome Decoding also appears unstructured, and the corresponding security assumption is seemingly conservative.

3.8. SDitH

Syndrome Decoding in the Head (SDitH) [21] follows the MPCitH framework and offers parameter sets using two optimization techniques. The hypercube variant uses additive secret sharing and has a method of converting a single protocol instance over 2^D parties into D instances over two parties. This variant yields smaller signatures with higher computational cost. The threshold variant, which was first presented in [22], uses low-threshold linear secret sharing and only requires the prover to reveal l parties' views instead of $N-1$ for some threshold l.

The security is based on the hardness of solving the d-split variant of the syndrome decoding problem for random linear codes over finite fields. When $d = 1$, the d-split variant is equivalent to SDP, which is known to be NP-hard and whose security is believed to be well-understood. The original SDitH specification overestimated security by a few bits due to multiple solutions to the syndrome decoding instances. The parameter sets were updated to ensure that the number of expected solutions is below 1.1.

The overall performance of SDitH can be seen as outperforming SLH-DSA but not ML-DSA or Falcon. SDitH features very small keys with signature sizes that fall between the SLH-DSA "small" and "fast" parameter sets. Although SDitH is closely related to a known NP-hard problem, NIST believes SDitH can benefit from more security analysis. Overall, SDitH is competitive with the other MPCitH candidates.

3.9. UOV

The Unbalanced Oil and Vinegar (UOV) digital signature scheme [23] is the oldest unbroken multivariate cryptosystem and was proposed in [24]. The construction of UOV is based on a system of quadratic equations for which there is a secret subspace on which the system evaluates to zero. This scheme offers EUF-CMA security following the hash-and-sign paradigm with this quadratic system and a salt using a construction similar to the one proposed by [25].

The performance advantages of UOV are its short signatures and very fast signing and verification speeds. UOV has also been a central object of study in multivariate cryptography for 25 years. However, a primary drawback of the scheme is the size of the public key. The submission package offers trade-offs between public key size and verification speed, but even the smaller public keys are quite large. For this reason, NIST anticipates that UOV

will primarily be applied to applications that require small signatures, fast verification, and offline transmission of the key.

While UOV is a mature and fairly stable scheme, an attack in the last four years marginally reduced the security of some of its parameter regimes [26]. NIST recommends that the community remain vigilant and continue to critically analyze the security of UOV.

3.10. MAYO

MAYO [27] is a variant of UOV with smaller public keys made by "whipping" a very small quadratic map into a larger one with a UOV structure [28]. This very small quadratic map is denoted here as *mini-UOV*. Thus, MAYO key recovery reduces to finding mini-UOV oil space, and MAYO signature forgery reduces to trying to invert the whipped UOV-like map. Thanks to this extra structure, MAYO significantly improves the public key size relative to UOV while inheriting UOV's small signature size. While it is not as fast as UOV, MAYO is still very efficient.

Recent results on solving underdetermined systems of multivariate equations [29] might slightly impact MAYO's security [30]. However, NIST maintains interest in MAYO for its competitive performance and encourages further research to assess whether the additional structure makes MAYO vulnerable to cryptanalysis.

3.11. QR-UOV

QR-UOV [31] is a variant of UOV with smaller public keys by using quotient rings with techniques from [32]. Unlike UOV matrices whose elements belong to a finite field $\mathbb{F}_q$, QR-UOV public matrices contain elements in a degree n field extension represented by a quotient ring. As a result, each $n \times n$ block in the public key uses only n coefficients, where n^2 would be needed in general. Thanks to this extra structure, QR-UOV public keys are 50 % smaller in comparison to UOV. While the performance of QR-UOV is slower than UOV, it is still competitive.

A previous attempt that relied on quotient rings was broken [33], and another candidate in the Additional Call for Digital Signatures that incorporated the same technique was also attacked [34, 35].

NIST maintains interest in QR-UOV for its competitive performance, but the structure of QR-UOV requires further study. NIST anticipates that the performance could be improved and encourages the designers to further optimize their implementation.

3.12. SNOVA

The SNOVA construction utilizes the well-studied design of UOV and adds extra structure to reduce the public key size. The SNOVA submission [36] is based on the SNOVA signature

scheme [37], which is a simplified version of the NOVA signature scheme [38] by the same authors.

SNOVA uses public matrices whose coefficients belong to a noncommutative ring, namely a ring of square matrices over a finite field. Thanks to this extra structure, SNOVA obtains significantly smaller public keys compared to UOV (comparable to or slightly smaller than those of MAYO) while still being relatively fast. SNOVA is a bit slower than MAYO but in the same range.

During the first round, SNOVA suffered an attack [39, 40] that affected some of the submitted parameter sets. In [41], SNOVA updated their parameters but then suffered a new attack [42]. Nonetheless, some of the submitted parameter sets of SNOVA survived both attacks, and it appears the remaining parameter sets can be patched to avoid the attacks with little effect on performance. Notably, the parameter sets that survived cryptanalysis were those with the smallest public keys for each security level.

The novelty of SNOVA and its history of attacks lead NIST to question its security even more so than the other structured-UOV schemes aimed at significantly reduced key size. Yet the fact that SNOVA still has unbroken parameter sets with the smallest public keys available for UOV-based schemes makes it an attractive candidate for continued study.

3.13. FAEST

FAEST [43] is a digital signature scheme constructed via a relatively new technique called VOLEitH [44]. This technique is related to the MPCitH approach [45] used by several other signature schemes in the NIST post-quantum standardization process. Both MPCitH and VOLEitH can be used to construct digital signature schemes whose unforgeability relies only on the security of some symmetric-key cipher E. In the case of FAEST, E is AES128, AES192, and AES256 for security levels 1, 3, and 5, respectively. A signing key of FAEST is then a key k of E, and a corresponding verification key is a pair (x, y) such that $E_k(x) = y$.

Just as with MPCitH, VOLEitH involves constructing an interactive ZKPoK based on certain computations with shares of the signing key and then compiling that ZKPoK into a non-interactive scheme via the Fiat-Shamir paradigm [46]. However, the computations involving the shares of the signing key are significantly different in VOLEitH and MPCitH. In the case of VOLEitH, these computations are based on a certain two-party primitive called Vector Oblivious Linear Evaluation. This results in FAEST having significantly smaller signatures compared to similar MPCitH schemes [43]. Moreover, the public keys of FAEST are very small (i.e., between 32 and 64 bytes), and the key generation, signing, and verification speeds are all competitive.

While the theoretical security of FAEST is based only on symmetric-key assumptions, its performance is significantly better than most other schemes with that property, including SLH-DSA [47]. However, the performance of FAEST is not competitive with lattice-based

schemes, such as ML-DSA and FN-DSA. FAEST is thus a promising scheme for applications that do not require the performance provided by lattice-based signatures.

The core technique of VOLEitH that underlies FAEST was introduced in 2023 [44]. The construction is somewhat complex, and the security proof is very technical. New results are appearing frequently in this active area. As a result, FAEST might undergo modifications in the near future. More work is needed for the scheme to stabilize and for the general community of cryptographers and cryptanalysts to become deeply familiar with and confident in the technical aspects of FAEST.

3.14. SQIsign

SQIsign [48] is a unique signature scheme that is designed using isogeny graphs of elliptic curves. Like several other candidates, SQIsign uses the Fiat-Shamir paradigm to turn a zero-knowledge identification scheme into a signature scheme. Security is based on the knowledge of a secret elliptic curve isogeny.

There has been a lot of recent activity related to the security of isogeny-based cryptosystems. Most notably, the KEM candidate SIKE [49] was shown to be vulnerable to efficient attacks that completely undermined its security claims [50–53]. Attempts to patch the vulnerabilities were ineffective [54]. As a result, more study is needed to establish greater confidence in isogeny-based schemes. SQIsign relies upon a different hardness assumption than SIKE, and consequentially, the aforementioned attacks do not work on SQIsign. Specifically, SIKE included additional information about the secret isogeny (i.e., the image of certain points) that were needed for key establishment. SQIsign uses new techniques that do not require this extra information to be shared.

SQIsign has the smallest combined size of public keys and signature sizes of all of the first-round candidates and even both ML-DSA and Falcon. In terms of computational efficiency of signing and verifying, SQIsign is noticeably slower than many of the other candidates, although verification is much faster than signing. New variants of SQIsign have been proposed with improved performance and a stronger security assumption compared to the originally submitted version [55, 56].

SQIsign is a very new design, and as such, will need more evaluation and analysis. NIST hopes that more research will lead to further optimizations that improve the performance of SQIsign, although it seems unlikely that signing will ever be competitive to the signing times of ML-DSA. However, SQIsign differs greatly from every other signature candidate, improving the diversity of security assumptions and performance profiles for the standardization process. Therefore, NIST advanced SQIsign to the second round.

4. Conclusion

The announcement of the 14 second-round candidates marks the start of the second round of the Additional Digital Signatures for the NIST PQC Standardization Process. This report summarized the evaluation criteria used to select these candidate algorithms, the basic designs of the second-round candidates, and their advantages and disadvantages. NIST greatly appreciates the participation in the NIST PQC Standardization Process.

Submitters of the second-round candidates will be allowed to adjust and improve their submissions to fix inconsistencies, problems, or shortcomings in the specifications or source code. Any changes must be submitted to NIST by January 17, 2025, in a complete submission package, as defined in [2]. More details will be provided on the pqc-forum [57] and the webpage https://csrc.nist.gov/projects/pqc-dig-sig.

Over the next several months, NIST invites the cryptographic community to evaluate the 14 second-round signature candidates. Some of the second-round candidates have received little or no published cryptanalysis by the cryptographic community-at-large. With the number of candidates substantially reduced from the first round, we hope that the combined efforts of the cryptographic community will evaluate the remaining candidates and provide NIST with feedback that supports or refutes the security claims of the submitters. NIST is also interested in additional performance data on each of the candidates, including optimized implementations written in assembly code or using instruction set extensions as well as analyses of the implementation suitability of candidate algorithms in constrained platforms and performance data for hardware implementations.

NIST plans to host another NIST PQC Standardization Conference in September 2025. Submitters of the second-round candidates will be invited to present their updated algorithms. In 2026, NIST plans to select finalists for a third round of evaluation. More detailed plans will be provided at a later date.

References

[1] Alagic G, Apon D, Cooper DA, Dang QH, Dang T, Kelsey JM, Lichtinger J, Liu YK, Miller CA, Moody D, Peralta R, Perlner RA, Robinson A, Smith-Tone D (2022) Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8413-upd1, Includes updates as of September 26, 2022. https://doi.org/10.6028/NIST.IR.8413-upd1

[2] National Institute of Standards and Technology (2022) Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf.

[3] Baldi M, Barenghi A, Bitzer S, Karl P, Manganiello F, Pavoni A, Pelosi G, Santini P, Schupp J, Slaughter F, Wachter-Zeh A, Weger V (2023) CROSS: Codes and Restricted Objects Signature Scheme, Submission to the NIST Post-Quantum Cryptography Standardization Process, Algorithm Specifications and Supporting Documentation. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/CROSS-spec-web.pdf.

[4] Baldi M, Barenghi A, andJean François Biasse LB, Esser A, Gaj K, Mohajerani K, Pelosi G, Persichetti E, Saarinen MJO, Santini P, Wallace R (2023) LESS: Linear Equivalence Signature Scheme. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/less-spec-web.pdf.

[5] Chou T, Persichetti E, Santini P (2023) On Linear Equivalence, Canonical Forms, and Digital Signatures, *Cryptology ePrint Archive preprint*. Available at https://ia.cr/2023/1533.

[6] Bos JW, Bronchain O, Ducas L, Fehr S, Huang YH, Porning T, Postlethwaite EW, Prest T, Pulls LN, van Woerden W (2023) HAWK, version 1.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/hawk-spec-web.pdf.

[7] Aragon N, Bardet M, Bidoux L, Chi-Domínguez JJ, Dyseryn V, Feneuil T, Gaborit P, Neveu R, Rivain M, Tillich JP (2023) MIRA Specifications. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MIRA-spec-web.pdf.

[8] Adj G, Rivera-Zamarripa L, Verbel J, Bellini E, Barbero S, Esser A, Sanna C, Zweydinger F (2023) MiRitH (MinRank in the Head). Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MiRitH_spec-web.pdf.

[9] Aguilar-Melchor C, Gama N, Howe J, Hülsing A, Joseph D, Yue D (2022) The Return of the SDitH, *Cryptology ePrint Archive preprint*. https://ia.cr/2022/1645.

[10] Rivain M (2024) Constructions for digital signatures part III: Threshold-computation-in-the-head. Available at https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/pqc-seminars/presentations/16-threshold-in-the-head-07022024.pdf.

[11] Bidoux L (2024) Merge of MIRA and MiRitH schemes, PQC-Forum Post. Available at https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/pAEqDYwhXqM/m/lOved79qAQAJ.

[12] Feneuil T, Rivain M (2023) MQOM: MQ on my Mind, Algorithm Specifications and Supporting Documentation (Version 1.0). Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MQOM-spec-web.pdf.

[13] Furue H, Kudo M (2024) Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings. *Post-Quantum Cryptography: 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part II* (Springer-Verlag, Berlin, Heidelberg), p 109–143. https://doi.org/10.1007/978-3-031-62746-0_6

[14] Aaraj N, Bettaieb S, Bidoux L, Budroni A, Dyseryn V, Esser A, Gaborit P, Kulkarni M, Mateu V, Palumbi M, Perin L, Tillich JP (2023) PERK. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/PERK-spec-web.pdf.

[15] Aragon N, Bardet M, Bidoux L, Chi-Domínguez JJ, Dyseryn V, Feneuil T, Gaborit P, Joux A, Rivain M, Tillich JP, Vinçotte A (2023) RYDE specifications. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf.

[16] Feneuil T (2024) Building MPCitH-Based Signatures from MQ, MinRank, and Rank SD. *Applied Cryptography and Network Security*, eds Pöpper C, Batina L (Springer Nature Switzerland, Cham), pp 403–431. https://doi.org/10.1007/978-3-031-54770-6_16

[17] Aguilar-Melchor C, Gama N, Howe J, Hülsing A, Joseph D, Yue D (2023) The Return of the SDitH. *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V* (Springer-Verlag, Berlin, Heidelberg), p 564–596. https://doi.org/10.1007/978-3-031-30589-4_20

[18] Feneuil T, Rivain M (2022) Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head, *Cryptology ePrint Archive preprint*. https://ia.cr/2022/1407.

[19] Feneuil T, Rivain M (2023) Threshold Computation in the Head: Improved Framework for Post-Quantum Signatures and Zero-Knowledge Arguments, *Cryptology ePrint Archive preprint*. https://ia.cr/2023/1573.

[20] Bidoux L, Feneuil T, Gaborit P, Neveu R, Rivain M (2024) Dual Support Decomposition in the Head: Shorter Signatures from Rank SD and MinRank, *Cryptology ePrint Archive preprint*. https://ia.cr/2024/541.

[21] Melchor CA, Feneuil T, Gama N, Gueron S, Howe J, Joseph D, Joux A, Persichetti E, Randrianarisoa TH, Rivain M, Yue D (2023) The Syndrome Decoding in the Head (SD-in-the-Head) Signature Scheme, Algorithm Specifications and Supporting Documentation – Version 1.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SDitH-spec-web.pdf.

[22] Feneuil T, Joux A, Rivain M (2022) Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs. *Advances in Cryptology – CRYPTO 2022*, eds Dodis

Y, Shrimpton T (Springer Nature Switzerland, Cham), pp 541–572. https://doi.org/10.1007/978-3-031-15979-4_19

[23] Beullens W, Chen MS, Ding J, Gong B, Kannwischer MJ, Patarin J, Peng BY, Schmidt D, Shih CJ, Tao C, Yang BY (2023) UOV: Unbalanced Oil and Vinegar, Algorithm Specifications and Supporting Documentation, Version 1.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/UOV-spec-web.pdf.

[24] Kipnis A, Patarin J, Goubin L (1999) Unbalanced Oil and Vinegar Signature Schemes. *Advances in Cryptology — EUROCRYPT '99*, ed Stern J (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 206–222. https://doi.org/10.1007/3-540-48910-X_15

[25] Sakumoto K, Shirai T, Hiwatari H (2011) On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack. *Post-Quantum Cryptography*, ed Yang BY (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 68–82. https://doi.org/10.1007/978-3-642-25405-5_5

[26] Beullens W (2021) Improved Cryptanalysis of UOV and Rainbow. *Advances in Cryptology – EUROCRYPT 2021*, eds Canteaut A, Standaert FX (Springer International Publishing, Cham), pp 348–373. https://doi.org/10.1007/978-3-030-77870-5_13

[27] Beullens W, Campos F, Celi S, Hess B, Kannwischer MJ (2023) MAYO. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/mayo-spec-web.pdf.

[28] Beullens W (2022) MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps. *Selected Areas in Cryptography*, eds AlTawy R, Hülsing A (Springer International Publishing, Cham), pp 355–376. https://doi.org/10.1007/978-3-030-99277-4_17

[29] Hashimoto Y (2023) An improvement of algorithms to solve under-defined systems of multivariate quadratic equations. *JSIAM Letters* 15:53–56. https://doi.org/10.14495/jsiaml.15.53

[30] Takeshi K, Beullens W (2024) Round 1 (Additional Signatures) OFFICIAL COMMENT: MAYO, NIST PQC Forum. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/MAYO-round1-dig-sig-official-comment.pdf.

[31] Furue H, Ikematsu Y, Hoshino F, Takagi T, Yasuda K, Miyazawa T, Saito T, Nagai A (2023) QR-UOV. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/qruov-spec-web.pdf.

[32] Furue H, Ikematsu Y, Kiyomura Y, Takagi T (2021) A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. *Advances in Cryptology – ASIACRYPT 2021*, eds Tibouchi M, Wang H (Springer International Publishing, Cham), pp 187–217. https://doi.org/10.1007/978-3-030-92068-5_7

[33] Furue H, Kinjo K, Ikematsu Y, Wang Y, Takagi T (2020) A Structural Attack on Block-Anti-Circulant UOV at SAC 2019. *Post-Quantum Cryptography*, eds Ding J, Tillich JP (Springer International Publishing, Cham), pp 323–339. https://doi.org/10.1007/978-3-030-44223-1_18

[34] Furue H (2023) Round 1 (Additional Signatures) OFFICIAL COMMENT: VOX, NIST PQC Forum. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/VOX-round1-dig-sig-official-comment.pdf.

[35] Guo H, Jin Y, Pan Y, He X, Gong B, Ding J (2024) Practical and Theoretical Cryptanalysis of VOX. *Post-Quantum Cryptography*, eds Saarinen MJ, Smith-Tone D (Springer Nature Switzerland, Cham), pp 186–208. https://doi.org/10.1007/978-3-031-62746-0_9

[36] Wang LC, Chou CY, Ding J, Kuan YL, Li MS, Tseng BS, Tseng PE, Wang CC (2023) SNOVA, Proposal for NISTPQC: Digital Signature Schemes project. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SNOVA-spec-web.pdf.

[37] Wang LC, Tseng PE, Kuan YL, Chou CY (2022) A Simple Noncommutative UOV Scheme, *Cryptology ePrint Archive preprint*. Available at https://ia.cr/2022/1742.

[38] Wang LC, Tseng PE, Kuan YL, Chou CY (2022) NOVA, a Noncommutative-ring Based Unbalanced Oil and Vinegar Signature Scheme with Key-randomness Alignment, *Cryptology ePrint Archive preprint*. Available at https://ia.cr/2022/665.

[39] Ikematsu Y, Akiyama R (2024) Revisiting the security analysis of SNOVA. *Proceedings of the 11th ACM Asia Public-Key Cryptography Workshop* APKC '24 (Association for Computing Machinery, New York, NY, USA), p 54–61. https://doi.org/10.1145/3659467.3659900

[40] Li P, Ding J (2024) Cryptanalysis of the SNOVA Signature Scheme. *Post-Quantum Cryptography*, eds Saarinen MJ, Smith-Tone D (Springer Nature Switzerland, Cham), pp 79–91. https://doi.org/10.1007/978-3-031-62746-0_4

[41] Team S (2024) Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA, NIST PQC Forum. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/SNOVA-round1-dig-sig-official-comment.pdf.

[42] Beullens W (2024) Improved Cryptanalysis of SNOVA, *Cryptology ePrint Archive preprint*. Available at https://ia.cr/2024/1297.

[43] Baum C, Braun L, de Saint Guilhem CD, Klooß M, Majenz C, Mukherjee S, Ramacher S, Rechberger C, Orsini E, Roy L, Scholl P (2023) FAEST: Algorithm Specifications, Version 1.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/FAEST-spec-web.pdf.

[44] Baum C, Braun L, de Saint Guilhem CD, Klooß M, Orsini E, Roy L, Scholl P (2023) Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head. *Advances in Cryptology – CRYPTO 2023*, eds Handschuh H, Lysyanskaya A (Springer Nature Switzerland, Cham), pp 581–615. https://doi.org/10.1007/978-3-031-38554-4_19

[45] Ishai Y, Kushilevitz E, Ostrovsky R, Sahai A (2007) Zero-Knowledge from Secure Multiparty Computation. *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing* STOC '07 (Association for Computing Machinery, New York, NY, USA), p 21–30. https://doi.org/10.1145/1250790.1250794

[46] Fiat A, Shamir A (1987) How To Prove Yourself: Practical Solutions to Identification and Signature Problems. *Advances in Cryptology — CRYPTO' 86*, ed Odlyzko AM (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 186–194. https://doi.org/10.1007/3-540-47721-7_12

[47] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

[48] Chavez-Saab J, Santos MCR, de Feo L, Eriksen JK, Hess B, Kohel D, Leroux A, Meyer M, Panny L, Patranabis S, Petit C, Henríquez FR, Schaeffler S, Wesolowski B (2022) SQISsign: Algorithm specifications and supporting documentation. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/sqisign-spec-web.pdf.

[49] Jao D, Azarderakhsh R, Campagna M, Costello C, de Feo L, Hess B, Hutchinson A, Jalali A, Karabina K, Koziel B, LaMacchia B, Longa P, Naehrig M, Pereira G, Renes J, Soukharev V, Urbanik D (2022) Supersingular Isogeny Key Encapsulation, Submission to the NIST's post-quantum cryptography standardization process. Available at https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/SIKE-Round4.zip.

[50] Castryck W, Decru T (2023) An Efficient Key Recovery Attack on SIDH. *Advances in Cryptology – EUROCRYPT 2023*, eds Hazay C, Stam M (Springer Nature Switzerland, Cham), pp 423–447. https://doi.org/10.1007/978-3-031-30589-4_15

[51] Maino L, Martindale C (2022) An attack on SIDH with arbitrary starting curve, *Cryptology ePrint Archive preprint*. https://ia.cr/2022/1026.

[52] Maino L, Martindale C, Panny L, Pope G, Wesolowski B (2023) A Direct Key Recovery Attack on SIDH. *Advances in Cryptology – EUROCRYPT 2023*, eds Hazay C, Stam M (Springer Nature Switzerland, Cham), pp 448–471. https://doi.org/10.1007/978-3-031-30589-4_16

[53] Robert D (2023) Breaking SIDH in Polynomial Time. *Advances in Cryptology – EUROCRYPT 2023*, eds Hazay C, Stam M (Springer Nature Switzerland, Cham), pp 472–503. https://doi.org/10.1007/978-3-031-30589-4_17

[54] Castryck W, Vercauteren F (2023) A Polynomial Time Attack on Instances of M-SIDH and FESTA. *Advances in Cryptology – ASIACRYPT 2023*, eds Guo J, Steinfeld R (Springer Nature Singapore, Singapore), pp 127–156. https://doi.org/10.1007/978-981-99-8739-9_5

[55] Dartois P, Leroux A, Robert D, Wesolowski B (2024) SQIsignHD: New Dimensions in Cryptography. *Advances in Cryptology – EUROCRYPT 2024*, eds Joye M, Leander G (Springer Nature Switzerland, Cham), pp 3–32. https://doi.org/10.1007/978-3-031-58716-0_1

[56] Basso A, Feo LD, Dartois P, Leroux A, Maino L, Pope G, Robert D, Wesolowski B (2024) SQIsign2D-West: The Fast, the Small, and the Safer, *Cryptology ePrint Archive preprint*. https://ia.cr/2024/760.

[57] (2024) NIST pqc-forum mailing list. Available at https://groups.google.com/a/list.nist.gov/g/pqc-forum.

Appendix A. List of Symbols, Abbreviations, and Acronyms

DNSSEC	Domain Name System Security Extensions
DSS	Digital Signature Standard
EUF-CMA	Existential Unforgeability under Chosen-Message Attack
FIPS	Federal Information Processing Standards
FN-DSA	FFT-Over-NTRU-Lattice-Based Digital Signature Algorithm; based on Falcon.
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ITL	Information Technology Laboratory
KEM	Key-Encapsulation Mechanism
LEP	Linear Equivalence Problem
ML-DSA	Module-Lattice-Based Digital Signature Algorithm; based on CRYSTALS-Dilithium.
ML-KEM	Module-Lattice-Based Digital Signature Algorithm; based on CRYSTALS-Kyber.
MPC	Multi-Party Computation
MPCith	Multi-Party Computation in the Head
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
omSVP	One More Shortest Vector Problem
OCSP	Online Certificate Status Protocol
PQC	Post-Quantum Cryptography
R-SDP	Restricted Syndrome Decoding Problem
R-SDP(G)	Restricted Syndrome Decoding Problem with subgroup G
SDP	Syndrome Decoding Problem
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm; based on SPHINCS$^+$.
smLIP	Search Module Lattice Isomorphism Problem
SP	Special Publication
SSH	Secure Shell
TLS	Transport Layer Security
UOV	Unbalanced Oil and Vinegar

VOLEitH	Vector Oblivious Linear Evaluation in the Head
ZKPoK	Zero-Knowledge Proof of Knowledge