NIST Internal Report
NIST IR 8610

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

Gorjan Alagic
Maxime Bros
Pierre Ciadoux
Quynh Dang
Thinh Hung 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.8610

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

NIST Internal Report
NIST IR 8610

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

Gorjan Alagic [1*], Maxime Bros [1†], Pierre Ciadoux [1‡], Quynh Dang [1], Thinh Hung Dang [1], John Kelsey [1], Jacob Lichtinger [1], Yi-Kai Liu [2], Carl Miller [1], Dustin Moody [1], Rene Peralta [1], Ray Perlner [1], Angela Robinson [1], Hamilton Silberg [1], Daniel Smith-Tone [1], Noah Waller [1]

[1] Computer Security Division, Information Technology Laboratory, NIST, Gaithersburg, Maryland, USA
[2] Applied and Computational Mathematics Division, Information Technology Laboratory, NIST, Gaithersburg, Maryland, USA

[*] NIST Associate (Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland, USA)
[†] NIST Associate (Foreign Guest Researcher, Contractor via Izum Inc.)
[‡] NIST Associate (Foreign Guest Researcher)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8610

May 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Technical Series Publications: https://www.nist.gov/nist-research-library/nist-publications

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.

References to Other Publications

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

Non-Endorsement Disclaimer

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.

Publication History

Approved by the NIST Editorial Review Board on 2026-05-05.

Suggested Citation

Gorjan Alagic, Maxime Bros, Pierre Ciadoux, Quynh Dang, Thinh Hung 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 (2026). Status Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Internal Report (IR) NIST IR 8610. DOI:10.6028/NIST.IR.8610

Author Names and ORCID Identifiers

Gorjan Alagic (0000-0002-0107-6037); Maxime Bros (0000-0001-7838-2529); Pierre Ciadoux (0009-0001-2272-681X); Quynh Dang (0009-0005-9801-6805); Thinh Hung 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).

Additional Information

Additional information about this publication, including related content, potential updates, and document history, is available at www.nist.gov/pqcrypto.

Contact Information: pqc-comments@nist.gov

Abstract

This report describes the evaluation criteria and selection process of the Second Round of the Additional Digital Signatures for the NIST Post-Quantum Cryptography (PQC) Standardization Process, which will identify 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 will 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. Based on public feedback and internal reviews of the second-round candidates, NIST has selected nine candidate algorithms to move forward to the third round of evaluation: FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, and UOV.

Keywords

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

Table of Contents

List of Tables

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. Proposed KEM and digital signature algorithms were submitted to NIST for consideration, and NIST narrowed down the submissions through a competition-like process. NIST selected four algorithms for standardization after three rounds of evaluation, and some algorithms moved on to a fourth round. One KEM and three digital signature schemes were selected at the end of the third round [1]. At the conclusion of the fourth round of the PQC Standardization Process, a KEM was selected for standardization [2].

NIST issued a new call for additional digital signatures in July 2022 to further diversify the PQC portfolio. While the initial post-quantum standards provide robust security, two of the signature schemes are based on structured lattices. Consequently, NIST sought additional general-purpose signature schemes based on a non-lattice security assumption as well as signature schemes optimized for short signatures and fast verification.

NIST published the Call for Proposals for Additional Digital Signatures [3], which specified the submission requirements and evaluation criteria, and received 50 submission packages in June 2023. Of those, NIST accepted 40 as first-round candidates, representing a broad array of different security assumptions. The submission packages of the first-round candidates were made available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures. After over a year of review, NIST selected 14 of the signature algorithms to move into the second round for further study [4].

The second round began on October 24, 2024, and continued until May 14, 2026. The Sixth NIST PQC Standardization Conference was held in Gaithersburg, Maryland, on September 24-26, 2025. The submission teams of the accepted second-round candidates were invited to present updates for their candidate algorithms. During the second round, these candidates were subjected to more detailed analysis by NIST and the broader cryptographic community. This analysis included continued research of the theoretical and empirical evidence used to justify the security of these cryptosystems, new implementations with improved performance, and the consideration of other factors that could aid or hinder the practical deployment of these cryptosystems. Throughout the second round, NIST received significant feedback from the cryptographic community. Based on public feedback and internal reviews of the candidates, NIST announced the selection of nine signature algorithms as third-round candidates in May 2026.

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 [3].
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 [4]. The public comment period for the second-round candidates began.
January 2025	Deadline for updated submission packages for the second round.
September 2025	The Sixth NIST PQC Standardization Conference was held in Gaithersburg, Maryland. Submission teams presented updates for their candidate algorithms.
May 2026	NIST announced the third-round candidates, and the public comment period on the third round began. NIST IR 8610, *Status Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process*, was released.

1.1. Purpose and Organization of This Document

This document is a report on the second round of the Additional Digital Signatures for the NIST PQC Standardization Process.

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

Section 3 summarizes each of the second-round candidates with brief descriptions of the algorithms, the properties of interest, and characteristics that might cause concern. It also presents the reasons why candidate algorithms were selected or not for the third round.

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

2. Evaluation Criteria and the Selection Process

2.1. Acceptance of the Second-Round Candidates

NIST accepted 14 candidate algorithms for the second round. Submission teams were allowed to make minor modifications and resubmit their updated packages, which had to meet the same requirements as the original submissions. One of the candidates was a merger of two first-round algorithms: Mirath (merged from MIRA and MiRitH). The complete updated specifications were posted on https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures on March 4, 2025, for public review. Table 2 lists the second-round digital signature candidates organized by category The candidates that were selected to advance to the third round are bold and in blue.

Table 2. Second-round digital signature candidates

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

2.2. Evaluation Criteria

NIST's Call for Proposals [3] 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 differ significantly from signature schemes that have already been selected by NIST for standardization. In particular, the Call for Proposals 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$^+$.

These criteria are further described below, along with a discussion of how they impacted the second-round candidate evaluations.

2.2.1. Security

Security remains 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, DNSSEC) and other applications (e.g., certificate transparency, document signing, code signing, firmware updates).

Submitters were encouraged but not required to provide proofs of security in relevant models. At a minimum, digital signature schemes need to enable existentially unforgeable signatures with respect to an adaptive chosen message attack (i.e., EUF-CMA security). However, a number of the submitted algorithms — and all of NIST's current and planned PQC standards for general-purpose signatures — target the more robust security definition of strong unforgeability with respect to an adaptive chosen message attack (SUF-CMA). NIST will continue to view SUF-CMA security as desirable.

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 [3] 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 attacks, multi-key attacks, and misuse. Submissions were encouraged to note additional desirable security properties beyond standard unforgeability (e.g., exclusive ownership, message-bound signatures, non-re-signability; see [5]). Finally, NIST required submission

packages to summarize known cryptanalytic attacks on the scheme and complexity estimates for these attacks.

During the second round, a number of candidates suffered significant attacks[6–11]. This was especially true of candidates in the multivariate category, which are all variants of Unbalanced Oil and Vinegar (UOV) [12]. The series of attacks on the multivariate candidates had the most significant effect on certain parameter sets of UOV, MAYO, and SNOVA. While these attacks bring the maturity of the UOV family of schemes into question, it should be noted that each of these schemes have parameter sets that have never been broken, including all of QR-UOV's proposed parameters. UOV, MAYO, and SNOVA have also proposed preliminary ideas to tweak or replace the broken parameter sets.

NIST expects each of the remaining candidates to navigate a different set of challenges. The schemes in the Multi-Party Computation in the Head (MPCitH) category are generally based on conservative security assumptions, but they have intricate designs and complex security proofs. Many of these were substantially revised during the second round to take advantage of recent research on techniques such as Threshold Computation in the Head (TCitH) and Vector Oblivious Linear Evaluation in the Head (VOLEitH). Establishing the confidence necessary for standardization will depend on the cryptographic community's ability to verify these proofs. While this is a nontrivial task, as shown by previous experience with standardization of the signature scheme SPHINCS+ [1], it will likely be easier if future scheme changes are fairly small. A primary challenge for HAWK and SQIsign will be a more complete understanding of their relatively novel security assumptions. While the underlying mathematical problems for both have been studied, NIST believes further analysis by a broader community would be helpful.

2.2.2. Cost and Performance

The second-most important factor when evaluating candidate signature algorithms is cost and performance. This includes the sizes of public keys, private keys, and signatures as well as the computational efficiency of key generation, signing, and verification operations. These evaluations also take into account random-access memory (RAM) requirements for software and gate counts for hardware. NIST 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.

During the transition from the first round to the second round, several signature schemes underwent significant changes to improve performance. Emerging techniques within the MPCitH category, such as TCitH and VOLEitH, led to improved signing and verification

operations and decreased signature sizes for the algorithms. VOLEitH was already incorporated in the first round version of FAEST. In the second round, all of the remaining MPCitH candidates also adopted one or both of these techniques and gained dramatic performance improvements. SQISign introduced architectural changes that accelerated signing and verification while reducing signature sizes. Second-round tweaks to LESS significantly reduced signature sizes through the use of canonical forms. While most other candidates also saw improvements through optimized implementations, these represented the most significant shifts in performance profiles during the second round.

2.2.3. Algorithm and Implementation Characteristics

The second round included candidates with unique designs and features that were not present in the previously selected algorithms. NIST prefers candidate algorithms with greater flexibility (e.g., capable of running efficiently on a wide variety of platforms, leverage parallelism or instruction set extensions to achieve higher performance). Simplicity remains a key factor, as it facilitates both security analysis and ease of adoption.

The community has contributed significant side-channel analyses, including research presented at the Sixth NIST PQC Standardization Conference [13–17]. While NIST is monitoring these findings — including both attacks and proposed defenses — no side-channel results in the second round were deemed decisive enough to eliminate a candidate. In most instances, implementing effective countermeasures at a reasonable cost appears feasible. NIST expects that efforts will continue to focus on achieving constant-time, side-channel-resistant implementations as these schemes mature in the third round.

Finally, NIST remains attentive to factors that could hinder or promote the adoption of an algorithm or implementation, such as intellectual property claims and licensing terms.

2.3. Selection of the Third-Round Candidates

NIST selected nine third-round candidates from the 14 second-round candidates using the evaluation criteria specified in [3] (see Table 3). NIST's candidate selection decisions were quite difficult at this stage due to the overall high quality of algorithms under consideration. In relative order of importance, NIST considered the security, cost and performance, and algorithm and implementation characteristics, of a candidate in selecting the third-round candidates. These considerations also took into account the differences between the candidates and existing digital signature standards, particularly with respect to security and performance profiles.

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 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.

Among the six second-round MPCitH candidates, NIST found most confidence in the security of FAEST and found MQOM to have the strongest performance numbers. SDitH offers algorithmic diversity and security based on the well-studied syndrome decoding problem for random linear codes. Though the MPCitH category was quite competitive, the performance profiles of the candidates overlapped sufficiently to allow NIST to focus on a select few. Thus, NIST selected FAEST, MQOM, and SDitH to move to the third round for additional analysis of their complex designs and security proofs.

Conversely, despite recent attacks on UOV, MAYO, and SNOVA, NIST has opted to keep all of the multivariate schemes under consideration during the third round because they provide distinct benefits. NIST's decision is informed by the long-standing history of UOV-based cryptography and the continued existence of unbroken parameter sets with promising performance profiles for each scheme. MAYO and SNOVA have the potential to be used as general-purpose signatures due to their small public-key sizes. UOV is the closest candidate to the original UOV cryptosystem, which has been studied for decades. QR-UOV is resistant to the wedge attack and its variants and also features public keys that are moderately smaller than those of UOV. Based on this recent cryptanalysis, NIST anticipates a longer timeline for the potential standardization of any of these multivariate schemes and is unlikely to standardize them without a further round of evaluation.

CROSS has small public keys but very large signatures, much like SLH-DSA. However, the underlying security problem of CROSS has a much shorter history of study than SLH-DSA's. CROSS also suffered an attack during the second round that led the team to update its parameters. This combination of security uncertainty and less competitive performance led to the elimination of CROSS. LESS features small signatures but very large public keys, and it is much slower than CROSS for key generation, signing, and verifying. LESS was also attacked during the second round, which brought the understanding of its security

into question. Though the small signatures of LESS are desirable, NIST did not select LESS to move forward to the third round.

Finally, HAWK and SQIsign were both selected to move to the third round. SQIsign has the smallest combined key and signature sizes among the candidates and adds to algorithmic diversity. While HAWK is lattice-based, it offers smaller signatures than Falcon and does not need floating-point arithmetic.

The algorithms that were not selected for the third round are no longer under consideration for standardization by NIST.

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

Lattice-Based	MPC-in-the-Head	Multivariate
HAWK	FAEST	UOV
	MQOM	MAYO
Isogeny-Based	SDitH	QR-UOV
SQIsign		SNOVA

3. Summary of the Second-Round Candidates

This section describes each of the second-round candidates, including their advantages and disadvantages. In addition, the discussion provides reasons why a scheme was or was not selected to advance to the third round. Submitters of advancing schemes may wish to address some of the provided suggestions for the third round.

3.1. CROSS

Codes and Restricted Objects Signature Scheme (CROSS) [18] is a Fiat-Shamir transform of a code-based identification scheme (CROSS-ID). The underlying hardness assumption in CROSS is the Restricted Syndrome Decoding (RSD) problem, which is a variant of the commonly used Syndrome Decoding (SD) problem.

CROSS-ID is a 5-round protocol in which one party proves to another that they possess a solution to an RSD problem without actually revealing that solution. The signature scheme is the result of applying a 5-round Fiat-Shamir transform to CROSS-ID using parallel repetition of CROSS-ID in order to amplify security.

CROSS has been the subject of additional security analysis since the first round. A security proof for the Fiat-Shamir transform used in CROSS was published during the second

round [6]. The same work presented an attack that led the CROSS submission team to change their parameters in their second-round tweak [6]. An issue with the existing security analysis of CROSS-ID (as presented in the security details document included in CROSS's second-round submission package) was also identified [19], although the author did not claim that this issue undermined the security of CROSS itself. In response, the CROSS team addressed the issue in an update of their security details document, which is available on their website [20].

The performance numbers for the current version of CROSS are comparable to those of SPHINCS+, with small keys and very large signatures. CROSS offers a slightly different profile with somewhat faster signing and somewhat larger public key sizes. Overall, NIST does not view the performance benefits of CROSS to be significant enough to keep it in consideration, particularly given the nature of the hardness assumptions of CROSS as compared to those of SPHINCS+. As a result, CROSS has been eliminated from moving to the third round.

3.2. LESS

Linear Equivalence Signature Scheme (LESS) [21] applies the Fiat-Shamir transform to a zero-knowledge proof system based on the Linear Code Equivalence (LCE) problem (also known as the Monomial Code Equivalence problem). This problem asks, given the row-reduced generator matrices, $\mathbf{G}_0, \mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$, for two codes that are equivalent up to permutation and scaling to recover the equivalence. That is, the goal is to write $\mathbf{G}_1 = \mathrm{RREF}(\mathbf{G}_0\mathbf{Q})$, where $\mathbf{Q} \in \mathbb{F}_q^{n \times n}$ is a monomial matrix (i.e., the product of a permutation matrix and a diagonal matrix).

LESS's second-round tweak significantly reduced signature sizes through the use of canonical forms [22] and other optimizations [23]. The resulting parameter sets have smaller signatures than those of the competing signature schemes (e.g., MPC, Threshold, VOLE-in-the-head-based) but still have much larger public-key sizes and fairly slow signing and verification. For example, parameter sets that target category 1 ranged from a 2,625 byte signature with a 13,940 byte public key to a 1,329 byte signature with a 97,484 byte public key.

During the second round, an attack was published on LESS [8], which reduced the concrete complexity of attacking LESS's parameter sets by amounts ranging from 12 bits for the category 1 parameters to 24 bits for the category 5 parameters. While this attack does not fundamentally alter the asymptotic complexity of attacking LESS, it suggests that LESS's parameter sets may fail to meet their security targets (at least if the cost of memory access

is ignored). There were also attacks published on related problems [24, 25] that did not have any immediate effect on LESS as submitted.

From a security perspective, the LCE problem is not as well-studied as the problems underlying some of its competitors (e.g., FAEST, SDitH, MQOM), and the recent attack of [8] brings the security of LESS's parameter choices into question. While LESS has an advantage over these schemes in terms of signature size, it also has significant disadvantages in terms of public-key size and signing and verification time. Ultimately, LESS was not selected.

3.3. SQIsign

SQIsign [26] is an isogeny-based signature scheme that relies on the presumed hardness of finding isogenies between supersingular elliptic curves and computing their endomorphism rings. The scheme functions as an identification protocol transformed into a signature scheme via the Fiat–Shamir transform. SQIsign is characterized by the smallest combined public-key and signature sizes of the second-round candidates. This makes it highly suitable for bandwidth-constrained environments, such as digital certificates and firmware updates.

During the second round, no classical or quantum polynomial-time attacks that threatened the core hardness assumptions of SQIsign were reported. In particular, SQIsign is resilient against the SIDH-related attacks that compromised the earlier isogeny-based key-exchange mechanism SIKE [2], since SQIsign avoids the auxiliary torsion-point information exploited by those attacks. SQIsign's signing procedure is mathematically intricate, making fully constant-time implementation challenging, though many of the underlying operations have been implemented in constant time. Recent analyses show that partial side-channel leakage could enable attacks and propose mitigations [27, 28]. By contrast, the verification procedure is simpler and much faster than signing.

Between rounds, SQIsign underwent a significant architectural refinement to improve efficiency and support a clearer security analysis [26]. The most notable design change was the move from the original KLPT-based path-finding algorithm to an approach that utilizes higher-dimensional isogenies. This change allows the response isogeny to be sampled from a more natural distribution, clarifying zero-knowledge properties and facilitating more complete formal security arguments in the random oracle model. The second-round submission also included updated parameter sets and optimizations to the internal representations of algebraic objects.

These refinements yielded substantial performance improvements: signing speeds increased by approximately 20 times and verification by a factor of six. Signature sizes were further

reduced, reaching as low as 148 bytes at security category 1. While SQIsign has higher latency than other candidates, its increased maturity and unique compactness led NIST to select it for the third round. Future efforts should prioritize the study of its security properties and potential performance optimizations with a particular focus on achieving fully constant-time signing to mitigate potential side-channel leakage.

3.4. HAWK

HAWK [29] is a lattice-based hash-and-sign signature scheme with some similarities to Falcon. Its design utilizes matrices over the same classes of cyclotomic rings found in other standardized lattice-based algorithms. A HAWK secret key consists of a randomly sampled, medium-sized basis $\mathbf{B}$ for the integer lattice that is algebraically structured so that it can be expressed as a rank-2 module. The HAWK public key is the corresponding Gram matrix $\mathbf{Q} = \mathbf{B}^*\mathbf{B}$, which gives the lengths and angles between the basis vectors but not their overall orientation in space. To sign a message, the signer hashes the message and a salt and uses the hash output h along with the secret $\mathbf{B}$ to determine a "secret" coset of the double-integer lattice from which a candidate short vector x is sampled. If x satisfies the norm bound, a signature s is generated from x, h, and $\mathbf{B}^{-1}$.

The signature consists of a salt used in the hashing and a compressed encoding of $\mathbf{s}$. The hardness of recovering the signing key relies on the presumed hardness of the Search Module Lattice Isomorphism Problem (smLIP) of rank 2, while unforgeability relies on the presumed hardness of the One-More-Shortest-Vector Problem (omSVP).

During the second round, significant cryptanalytic results were published regarding HAWK's underlying assumptions. Specifically, research in [30] identified a discrepancy in the original definition of the omSVP problem used in the first-round security proof. While these findings did not enable practical forgeries or compromise the scheme's concrete security, the second-round submission included a refined problem definition that explicitly excludes the identified attack vectors. Furthermore, while advancements in solving variants of the smLIP problem were made in [30, 31], these techniques currently appear inapplicable to the complex cyclotomic number fields utilized by HAWK. Additional cryptanalysis in [32, 33] further explored the hardness of these underlying module problems, showing that the choice of the underlying ring can strongly affect security.

HAWK offers a highly efficient performance profile with signatures of size 555 bytes at security category 1, which is smaller than Falcon or ML-DSA. Beyond its competitive size, HAWK's primary advantage over Falcon is its reliance on integer-only arithmetic. By eliminating the complicated floating-point operations required by Falcon, HAWK facilitates

easier implementation and better performance on constrained hardware platforms that lack dedicated floating-point units.

NIST selected HAWK for the third round due to its strong performance and because its implementation only needs integer arithmetic operations. NIST encourages further analysis of HAWK's security assumptions, particularly the smLIP problem within the specific structure of cyclotomic number fields.

3.5. FAEST

FAEST [34] is a signature scheme constructed using the VOLE-in-the-Head framework for building zero-knowledge proofs [35]. It utilizes the QuickSilver protocol [36] to prove low-degree constraints. The ideal VOLE functionality allows the prover to input a witness and distributes VOLE correlations between the prover and the verifier, which then allow the prover to prove low-degree constraints on the witness. In particular, the witness is either an extended AES key or plaintext, depending on whether the Even-Mansour variant is used, and the constraints are defined via the AES cipher. This VOLE functionality can be instantiated using oblivious transfer (OT) via the SoftSpokenVOLE construction [37]. Furthermore, the VOLE-in-the-head technique replaces OT with a commitment scheme using symmetric primitives, such as hash functions or pseudorandom generators (PRGs). Although commitments do not inherently protect the privacy of the verifier's input as OT does, FAEST arranges the protocol so that all of the verifier's OT inputs and outputs are deferred to the final rounds. Consequently, verifier privacy is not required for security, resulting in a proof system based entirely on well-established symmetric primitives. Interestingly, both descriptions of VOLEitH and TCitH frameworks have recently been subsumed under the formalism of Polynomial Interactive Oracle Proofs (PIOP) [38].

In the second round, FAEST was updated to improve performance, and additional security analysis was provided. Notable algorithmic changes include the "one-tree-to-rule-them-all" technique [39], a switch to an AES-based PRG for the commitment scheme, and a refined method for proving AES constraints using degree-3 polynomials within the QuickSilver framework. These architectural shifts necessitated updated security reductions, including new proofs in the Quantum Random Oracle Model (QROM) [40, 41].

Recent cryptanalytic work also explored the physical security of FAEST, specifically identifying new side-channel and fault-injection attacks against a masked implementation [42]. Several countermeasures were also proposed in the same work. While these findings underscore the need for further study of physical attack vectors — a challenge common to many second-round candidates — they do not undermine the scheme's fundamental security.

NIST selected FAEST to advance to the third round based on its distinct security assumptions and competitive performance among the VOLE/MPC-in-the-Head candidates. Its security relies primarily on well-established symmetric primitives, and while the specific properties required of these primitives are somewhat unconventional, the overall design is considered conservative.

3.6. Mirath

Mirath [43] is an MPCitH-based signature scheme resulting from the merger of two first round candidates: Mira [44] and MiRitH [45]. The security of Mirath relies on the hardness of finding a non-trivial, low-rank linear combination of matrices over a finite field, known as the MinRank Problem. For the second round, Mirath was revised to take advantage of recent progress in MPCitH techniques, specifically using TCitH techniques with an optional variant using the VOLEitH framework. Mirath was also updated to support dual support modeling [46], which relies on the equivalent MinRank Syndrome problem to decrease signature size.

During the second round, Mirath's security was further evaluated through both classical and quantum lenses. Recent analysis in [47] explored "partial key exposure" attacks on rank-based schemes, refining the understanding of security margins under secret key leakage. Furthermore, new research [48] provided a SUF-CMA security proof in the QROM, tightening the gap between traditional and quantum security bounds to offer more robust guarantees than the initial submission.

In terms of performance, the submitters introduced refined parameter sets during the second round that improved key generation, signing, and verification speeds by up to a factor of 10 [49]. However, despite these substantial gains and the maturity of the MinRank assumption, NIST has not chosen to move Mirath into the third round. This decision is primarily due to the competitive field of candidates within the MPCitH category. NIST chose to prioritize a smaller selection of such candidates that offer more established security (e.g., relying only on AES) or a superior performance profile relative to the remaining MPCitH/TCitH/VOLEitH options.

3.7. MQOM

MQOM [50] is a digital signature scheme based on the MPCitH paradigm. The underlying computational assumption is the hardness of solving random multivariate systems of quadratic equations over a finite field (i.e., the MQ problem). Like other MPCitH schemes, MQOM has been revised to take advantage of significant recent advances in the field.

The second-round version of MQOM is based on the TCitH specialization of MPCitH [51], although it could alternatively be viewed as using VOLEitH. In the TCitH paradigm, the typical additive secret sharing is replaced with threshold Shamir secret sharing. When combined with other recently developed MPCitH optimizations, this approach can yield significant reductions in signature sizes.

The current version of MQOM has a highly competitive performance profile that could be practical for a wide range of applications. At all three security levels, it offers the smallest total public-key and signature sizes among all six MPCitH candidates. In addition, the cycle counts of signing and verification are very competitive with those of the other candidates' comparable parameter sets. Due to its performance profile and the relative stability of the underlying hard problem, MQOM was selected to advance to the third round.

Like the other schemes that have undergone significant recent changes, MQOM will require careful further analysis. Currently, security proofs of MQOM in the Random Oracle Model (ROM) and QROM might not be considered mature or complete. Of particular interest to NIST is continued refinement of the provable analysis of MQOM security, particularly in models that capture the power of quantum attackers [48, 52, 53].

3.8. PERK

PERK [54] is a signature scheme based on a zero-knowledge proof of knowledge (ZKPoK) of a secret permutation. Given a matrix $\mathbf{H}$ and an array $\mathbf{x}$, the signatory proves knowledge of a permutation π such that $\pi(\mathbf{x})$ is in the kernel of H (i.e., $\mathbf{H}\pi(\mathbf{x}) = 0$). The security assumption, called the Permuted Kernel Problem (PKP), 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 MPCitH techniques, specifically the VOLEitH framework [55]. For the second round, the submission was reverted to the standard PKP assumption to address concerns regarding the non-standard variants used in the first round. Although the PKP assumption was proposed around 30 years ago, there is not much cryptanalytic literature on the subject. Some progress was made during the second round [56], but this did not affect the parametrization of PERK.

As with the other MPCitH schemes, the underlying techniques for building the ZKPoK were vastly improved in the second round. The second-round version also improved on the representation of the permutation matrix encoding π. These optimizations, added in an update to their second round submission, achieve a significant reduction in the length of the signature on the order of approximately 40%. Even with these improvements, however, PERK is significantly slower than FAEST, although PERK signatures are about

10 percent smaller than FAEST signatures. The slight advantage in signature size is offset by a substantial disparity in computational efficiency versus some of its competitors. In particular, FAEST offers superior speed and relies solely on AES. Therefore, NIST did not select PERK to advance to the third round. This decision was based on these practical performance trade-offs and should not be interpreted as a lack of confidence in the underlying Permuted Kernel Problem.

3.9. RYDE

RYDE [57] is a digital signature algorithm built on the MPCitH paradigm. Its underlying problem is a variant of the Rank Syndrome Decoding (RSD) problem called RSD_S. In the second-round specification and a later update [58], RYDE's changes significantly improved the performance of implementations for the "short" parameter sets. The primary change was moving to TCitH, and the end result reduced signature sizes by roughly half across all parameter sets.

While RYDE's RSD_S problem is less studied than other underlying MPCitH problems, some analysis has been done. The security of RYDE's specific RSD variant was further clarified during the second round through its formal reduction to the base RSD problem [46]. Furthermore, recent theoretical work [48] has incorporated RYDE's second-round optimizations into a formal security proof, strengthening its standing.

RYDE's performance profile is most similar to MQOM and Mirath, and all three have category 1 signature sizes between 3 and 3.5 kilobytes. Of the MPCitH schemes, these are generally the smallest signatures. Of those three, MQOM has consistently faster implementation speed when comparing similar sized parameters.

The second-round MPCitH candidates all utilized similar improvements (e.g., moving to TCitH or VOLEitH with additional generic optimizations) that resulted in similar core structures, performance profiles, and general security properties. While NIST finds the performance profile and security of MPCitH schemes promising in terms of possible standardization, NIST chose to narrow down to a smaller group of MPCitH candidates in this round. To avoid standardizing multiple schemes with very similar operational trade-offs, NIST chose to prioritize candidates that demonstrated the most robust combination of performance and community-wide analysis. As a result, despite its improvements during the second round, RYDE was not selected to advance.

3.10. SDitH

Syndrome Decoding in the Head (SDitH) [59] is a digital signature scheme based on the hardness of the syndrome decoding problem for random linear codes over finite fields. SDitH uses MPC-in-the-Head techniques, starting with an interactive identification protocol, which is transformed into a signature scheme via the Fiat-Shamir heuristic.

Recently, there has been dramatic progress in improving the efficiency of MPC-in-the-Head schemes using techniques such as VOLE-in-the-Head [35] and Threshold Computation in the Head [51]. Like many candidates in this category, SDitH has been redesigned to incorporate these advances using arithmetic encoding of the syndrome decoding problem and VOLE techniques [55, 60].

One strength of SDitH is its hardness assumption, which is generally considered more conservative than those used in other MPCitH schemes with the obvious exception of FAEST. This is due to the use of unstructured linear codes over the binary field, a problem that has been extensively studied [61]. However, while SDitH can be tuned to have competitive key and signature sizes, it typically incurs a higher computational cost compared to its peers.

Like other MPCitH schemes, SDitH has a complicated design, which has been substantially revised during the past two years. It will be important for SDitH and other MPCitH schemes to receive sufficient analysis by the cryptographic community in order to identify any design flaws that may affect their security as well as bugs in their security proofs. For this reason, NIST decided to reduce the number of MPCitH schemes to receive a greater focus from the community on a smaller number of more promising standardization candidates. NIST selected SDitH to continue to the third round of the evaluation process due to its hardness assumption, which is one of the most conservative among its peers.

3.11. UOV

The Unbalanced Oil and Vinegar (UOV) scheme is a foundational multivariate designs from the 1990s. The submission to the NIST process [62] is based on this well-studied framework, which is primarily distinguished by its specific parameter selections and the implementation of generic key compression techniques. The selection of UOV as a second-round candidate reflects its historical resilience against cryptanalysis and its value in expanding the algorithmic diversity of candidates. UOV also offers an attractive performance profile for some applications, such as very short signatures with fast verification.

UOV utilizes a structured system of quadratic polynomials that vanishes on a secret subspace. This structure allows for the efficient calculation of preimages via affine

projection and the solution of a small linear system. With this construction, UOV can achieve digital signatures as small as 96 bytes in size at security category 1 with verification in the tens of thousands of cycles on some benchmarking platforms. The cost of this approach, however, is public keys over 200 kilobytes in expanded form. As a result, NIST is primarily interested in UOV's suitability for certain applications rather than as a general-purpose signature scheme.

During the second round, UOV was subject to a new "wedge attack" [9] that used exterior products to expose the hidden secret subspace. This analysis affected the security margins of three out of four proposed parameter sets, and security reductions ranged from a few bits (category 1) to approximately 20 bits (category 5). A subsequent attack [11] further exploited small field characteristics, bringing the same three parameter sets (i.e., uov-Ip, uov-III, and uov-V) below their target security strengths.

While second-round analysis identified weaknesses in characteristic-2 and small-field implementations, these results primarily informed parameter selection rather than invalidating the UOV construction itself. With proper reparameterization, UOV should be able to meet its target security strengths. Furthermore, the general UOV construction remains a conservative choice, as a fundamental attack on its structure would likely imply an attack on all multivariate candidates. By advancing UOV, NIST ensures the continued availability of a small-signature, fast-verification option that provides algorithmic diversity.

Moving forward, the UOV submission team may wish to consider refining their parameter selection in light of recent exterior product and small-field attacks [9, 11]. Since odd-characteristic UOV appears resilient to these specific techniques [63], exploring odd-characteristic parameters may offer a more robust path toward optimal performance and security margins in the third round. The UOV team may also consider evaluating the inclusion of salt-UOV. While designed to achieve provable EUF-CMA security by avoiding statistical leakage, the repeated sampling process introduces potential timing side-channels that may offset its architectural benefits.

3.12. MAYO

MAYO [64] is a variant of the UOV framework that utilizes a public "whipping" algorithm to expand a small, structured public key (mini-UOV) into a larger structured UOV instance. Signing is then accomplished as in UOV. The key difference in the structure of this full UOV instance compared to traditional UOV is that each quadratic form has a block structure in which all blocks are permutations of a block defined by the mini-UOV instance. To date, no attack has been published that explicitly exploits the combination of this "whipping" structure with the mini-UOV structure generating these blocks.

During the second round, a wedge attack that affects characteristic 2 UOV-based schemes was presented [9]. The impact of the attack on perceived security was significant for the MAYO_2 parameters that targeted security category 1, resulting in a deficiency of roughly 30 bits. As specified in [9], the greater effect on MAYO in comparison to category 1 UOV seems to be due to the balance of the number of quadratic forms compared to the codimension of the secret subspace, not the "whipping" structure of the scheme.

MAYO has an interesting mixture of performance characteristics. In terms of public-key size, which is typically the greatest drawback of multivariate schemes, the MAYO parameter sets offer some of the smallest options among the multivariate candidate schemes. The MAYO_2 parameter set offers signature sizes that are about average among the UOV-based family at a cost of public-key sizes that are roughly three times as large as MAYO_1. The MAYO_1, MAYO_3, and MAYO_5 parameter sets offer the largest signature sizes among current multivariate candidates at their respective security levels. At the same time, MAYO retains efficiency in signing and verification, as expected from UOV-based schemes. With this balance in performance, the scheme is reasonable to consider as a general-purpose digital signature scheme.

While the wedge product attack had a significant effect on one of the security category 1 parameter sets, the effectiveness of the attack seems related to the shape of the instance, which is tuned for optimizing different aspects of performance, and not the inherent design philosophy of the scheme. MAYO remains attractive for its balanced parameter sets and offers gains over traditional UOV in public-key size while retaining signing and verification efficiency. For this reason, NIST has chosen to advance MAYO into the third round while acknowledging that the effect of the wedge attack on MAYO_2 underscores the risks associated with parameter selection for such schemes.

As in the case of UOV, MAYO should ensure that parameters are secure against recent exterior product and small-field attacks [9, 11]. It may be worthwhile to consider odd characteristic parameter sets as a countermeasure to these sorts of attacks. Similar considerations also apply to those mentioned in the UOV section with respect to a possible salt-UOV variant of MAYO.

3.13. QR-UOV

QR-UOV [65] is a variant of UOV that achieves smaller public keys by using quotient rings with techniques from [66]. Unlike traditional UOV, where matrix elements belong to a finite field $\mathbb{F}_q$, QR-UOV public matrices contain elements in a degree ℓ field extension (represented by a quotient ring). As a result, each $\ell \times \ell$ block in the public key uses only ℓ coefficients, where ℓ^2 would be needed in general. QR-UOV public-key sizes are

approximately 15–50% of standard UOV's because of this extra structure. While this reduction is less aggressive than that of MAYO or SNOVA, it inspires greater confidence regarding its security margins. Recent improvements [65, 67] offer performance similar to that of the compressed version of UOV.

A significant advantage of QR-UOV during the second round was its resilience to the wedge attack [9]. Because the attack primarily targets UOV-based schemes over fields of characteristic 2, QR-UOV's use of odd-characteristic fields rendered it unaffected. Although the attack was later extended to odd characteristics [63], its complexity remains higher than existing attacks on the scheme, and subsequent cryptanalysis [11, 68] has not diminished its security profile.

One difference between QR-UOV and other UOV-based schemes is how values are resampled during signing. In UOV, the target vector is fixed, and vinegar variables are sampled until the linear map used to solve for the oil variables is invertible. This prevents UOV from being proven EUF-CMA secure, since there is a bias on the vinegar variables that depend on secret information. However, no known practical attack takes advantage of this bias. In contrast, QR-UOV samples the vinegar variables once and then resamples the target vector until there is a solution. This avoids a biased distribution for the vinegar variables but is likely to be very costly to implement in a way that protects against timing side-channel attacks.

The second-round submission displays large performance improvements. With similar parameters, signing and verification speeds are approximately 15 to 20 times faster than the first-round version, while public-key and signature sizes stayed the same. There were also some further improvements in [67]. Comparing this implementation for small values of ℓ to compressed UOV, key generation is slightly faster, signing is three to five times faster, and verification is half as fast. Expanded UOV is faster, especially for signing, but QR-UOV does not offer an expanded version.

Overall, QR-UOV offers some significant public-key size reductions compared to UOV. While the public keys are still larger than those for MAYO and SNOVA, no attacks have decreased QR-UOV's security during the second round. As a result, QR-UOV has been selected to move to the third round.

3.14. SNOVA

SNOVA [69] is a variant of UOV that adds additional structure in order to reduce the public-key size. Of the four UOV variants in the second round, SNOVA exhibits the most aggressive public-key size reduction.

SNOVA was designed using concepts from non-commutative rings. However, it can also be characterized as applying a similar whipping transformation to that of MAYO to a structured UOV public key [70]. The main structural feature designed to further reduce SNOVA's public-key size below the sizes achieved by MAYO is that its oil space can be expressed using a basis matrix that consists of $\ell \times \ell$ blocks, which are restricted to lie in a matrix ring isomorphic to $\mathbb{F}_{q^\ell}$, as denoted $F_q[\mathbf{S}]$ by the SNOVA specification document. This allows each of SNOVA's public-key polynomials to implicitly represent a family of ℓ^2 related UOV polynomials that are related by blockwise left or right multiplication by the matrix $\mathbf{S}$.

SNOVA has a concerning history of cryptanalysis. In addition to several attacks suffered in the first round [70–72], SNOVA has also suffered additional attacks in the second round [7, 10, 11]. Of these, [10], a variant of the wedge attack [9] is particularly concerning, since it broke most of SNOVA's proposed parameter sets, often by a large margin. In response, the SNOVA team has proposed a modification using odd characteristic fields and by specifying its public-key using symmetric quadratic forms rather than asymmetric bilinear forms [73]. They instantiated this modification with a proposed parameter set targeting category 1 security, whose performance is highly competitive: the public-key and signature sizes are both smaller than those of Falcon, the highest-performing lattice-based signature scheme previously selected by NIST for standardization [1]. Similarly competitive parameters in both even and odd characteristic fields were later proposed in [74] for a variant of SNOVA that was reformulated to have a more flexible parameter space.

Despite its concerning history of cryptanalysis, SNOVA still seems to offer the possibility of a general-purpose signature scheme with fast verification and very small signatures and public keys, as illustrated by some of the originally proposed and unbroken parameter sets and new parameter sets proposed in [73, 74]. As such, NIST believes this possibility remains worth exploring, and is keeping SNOVA to move to the third round. NIST does not see SNOVA as having reached a stable form, and will consider more significant tweaks than it would for more mature schemes but will conversely require a longer time frame to consider moving any variant of SNOVA to standardization.

4. Conclusion

This announcement of the nine third-round candidates marks the start of the third round of the Additional Digital Signatures for the NIST PQC Standardization Process. This report summarizes the evaluation criteria used to select these candidate algorithms, the

basic designs of the second-round candidates, their advantages and disadvantages, and reasons why a candidate was (or was not) selected.

Submitters of the third-round candidates will be allowed to adjust and improve their submissions to address inconsistencies, problems, or shortcomings in the specifications or source code. Any changes must be submitted to NIST by August 14, 2026 in a complete submission package, as defined in [3]. As a general guideline, NIST expects any modifications to be relatively minor, except where explicitly called for by NIST in Sec. 3. Significant changes may signal that an algorithm is not mature enough for standardization at this time. More details will be provided on the pqc-forum [75] and webpage https://csrc.nist.gov/projects/pqc-dig-sig.

Over the next several months, NIST invites the cryptographic community to evaluate these nine third-round signature candidates. With the number of candidates reduced, NIST hopes for 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, 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 the first half of 2027. Submitters of the third-round candidates will be invited to present their updated algorithms. More detailed plans will be provided at a later date. NIST greatly appreciates participation in the NIST PQC Standardization Process.

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. DOI:10.6028/NIST.IR.8413-upd1

[2] Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu YK, Miller C, et al. (2025) Status Report on the Fourth 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 8545. DOI:10.6028/NIST.IR.8545

[3] 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.

[4] National Institute of Standards and Technology (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), DOI:10.6028/NIST.IR.8528

[5] Cremers C, Düzlü S, Fiedler R, Janson C, Fischlin M (2021) BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures. *2021 IEEE Symposium on Security and Privacy (SP)* (IEEE Computer Society, Los Alamitos, CA, USA), pp 1696–1714. DOI:10.1109/SP40001.2021.00093

[6] Battagliola M, Longo R, Pintore F, Signorini E, Tognolini G (2025) A revision of CROSS security: Proofs and attacks for multi-round Fiat–Shamir signatures: M. battagliola et al. *Mediterranean Journal of Mathematics* 22(5):132. DOI:10.1007/s00009-025-02882-7

[7] Cabarcas D, Li P, Verbel JA, Villanueva-Polanco R (2025) Improved attacks for SNOVA by exploiting stability under a group action. *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part VI*, eds Kalai YT, Kamara SF (Springer), *Lecture Notes in Computer Science*, Vol. 16005, pp 358–389. DOI:10.1007/978-3-032-01887-8_12. Available at https://doi.org/10.1007/978-3-032-01887-8_12

[8] Budroni A, Esser A, Franch E, Natale A (2025) Two is all it takes: Asymptotic and concrete improvements for solving code equivalence, Cryptology ePrint Archive, Paper 2025/227. Available at https://eprint.iacr.org/2025/227.

[9] Ran L (2025) Wedges, oil, and vinegar – an analysis of UOV in characteristic 2, Cryptology ePrint Archive, Paper 2025/1143. Available at https://eprint.iacr.org/2025/1143.

[10] Bros M, Le TH, Lichtinger J, Minaud B, Perlner R, Smith-Tone D, Valenzuela C (2026) Exploiting SNOVA's structure in the wedge product attack, Cryptology ePrint Archive, Paper 2026/237. Available at https://eprint.iacr.org/2026/237.

[11] Furue H, Ikematsu Y (2026) Key recovery attacks on UOV using p^l-truncated polynomial rings, Cryptology ePrint Archive, Paper 2026/298. Available at https://eprint.iacr.org/2026/298.

[12] 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. DOI:10.1007/3-540-48910-X_15

[13] Godard J, Aragon N, Gaborit P, Loiseau A, Maillard J (2025) Single trace side-channel attack on the MPC-in-the-Head framework. *Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8-10, 2025, Proceedings, Part II*, eds Niederhagen R, Saarinen MO Lecture Notes in Computer Science (Springer), pp 267–293. DOI:10.1007/978-3-031-86602-9_10. Available at https://doi.org/10.1007/978-3-031-86602-9_10

[14] Melissa Azouaoui (2025) Recent Contributions to the Physical Security of ML-DSA. Available at https://csrc.nist.gov/csrc/media/presentations/2025/recent-contributions-to-the-physical-security-of-m/recent_contributions-azouaoui_1-10.pdf.

[15] Elie Eid (2025) Masking FrodoKEM. Available at https://csrc.nist.gov/csrc/media/presentations/2025/masking-frodokem/masking_frodokem-eid_1.9.pdf.

[16] Mahmudul Faisal AL Ameen (2025) Systematic Timing Leakage Analysis of NIST PQDSS Candidates: Tooling and Lessons Learned. Available at https://csrc.nist.gov/csrc/media/presentations/2025/systematic-timing-leakage-analysis-(1)/systematic_timing_leakage_analysis-al-ameen_1.11%20.pdf.

[17] Kundu S, Norga Q, Karmakar A, Ojha UK, Ganguly A, Verbauwhede I (2025) mUOV: Masking the unbalanced oil and vinegar digital signature scheme at first- and higher-order. *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, CCS 2025, Taipei, Taiwan, October 13-17, 2025*, eds Huang C, Chen J, Shieh S, Lie D, Cortier V (ACM), pp 1994–2008. DOI:10.1145/3719027.3765188. Available at https://doi.org/10.1145/3719027.3765188

[18] Baldi M, Barenghi A, Battagliola M, Bitzer S, Gianvecchio M, Karl P, Manganiello F, Pavoni A, Pelosi G, Pintore F, Santini P, Schupp J, Signorini E, Slaughter F, Wachter-Zeh A, Weger V (2025) CROSS: Codes and Restricted Objects Signature Scheme. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/cross-spec-round2-web.pdf.

[19] Levin S (2025) A note on zero-knowledge simulator of the CROSS identification protocol, Cryptology ePrint Archive, Paper 2025/359. Available at https://eprint.iacr.org/2025/359.

[20] Baldi M, Barenghi A, Battagliola M, Bitzer S, Gianvecchio M, Karl P, Manganiello F, Pavoni A, Pelosi G, Pintore F, Santini P, Schupp J, Signorini E, Slaughter F, Wachter-Zeh A, Weger V (2025) CROSS: Codes and Restricted Objects Signature Scheme: Security Details. Version 2.2 - July 31, 2025. Available at https://www.cross-crypto.com/CROSS_SecurityDetails_v2.2.pdf.

[21] Baldi M, Barenghi A, Beckwith L, Biasse JF, Chou T, Esser A, Gaj K, Karl P, Mohajerani K, Pelosi G, Persichetti E, Saarinen MJO, Santini P, Wallace R, Zweydinger F (2025) LESS: Linear Equivalence Signature Scheme. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/less-spec-round2-web.pdf.

[22] Chou T, Persichetti E, Santini P (2025) On linear equivalence, canonical forms, and digital signatures. *Des Codes Cryptogr* 93(7):2415–2457. DOI:10.1007/S10623-025-01576-1. Available at https://doi.org/10.1007/s10623-025-01576-1

[23] Beckwith L, Esser A, Persichetti E, Santini P, Zweydinger F (2025) LESS is even more: Optimizing digital signatures from code equivalence, Cryptology ePrint Archive, Paper 2025/1424. Available at https://eprint.iacr.org/2025/1424.

[24] Nowakowski J (2024) An improved algorithm for code equivalence, Cryptology ePrint Archive, Paper 2024/1272. Available at https://eprint.iacr.org/2024/1272.

[25] Battagliola M, Mora R, Santini P (2025) Using the Schur product to solve the code equivalence problem, Cryptology ePrint Archive, Paper 2025/1017. Available at https://eprint.iacr.org/2025/1017.

[26] Aardal MA, Adj G, Aranha DF, Basso A, Martínez IAC, Chávez-Saab J, Santos MCR, Dartois P, Feo LD, Duparc M, Eriksen JK, Fouotsa TB, Filho DLG, Hess B, Kohel D, Leroux A, Longa P, Maino L, Meyer M, Nakagawa K, Onuki H, Panny L, Patranabis S, Petit C, Pope G, Reijnders K, Robert D, Henríquez FR, Schaeffler S, Wesolowski B (2025) Algorithm specifications and supporting documentation Version 2.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/sqisign-spec-round2-web.pdf.

[27] Basso A, Feo LD, Méaux P, Pintore F (2023) SQIsign: compact post-quantum signatures from isogenies and lattices, Cryptology ePrint Archive, Paper 2023/807. https://ia.cr/2023/807.

[28] Mukherjee A, Czuprynko M, Jacquemin D, Kutas P, Roy SS (2025) Simple power analysis attack on SQIsign, Cryptology ePrint Archive, Paper 2025/830. https://ia.cr/2025/830.

[29] 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.

[30] Luo H, Jiang K, Pan Y, Wang A (2024) Cryptanalysis of rank-2 module-LIP with symplectic automorphisms, Cryptology ePrint Archive, Paper 2024/1173. Available at https://eprint.iacr.org/2024/1173.

[31] van Gent DMH, Pulles LN (2025) HAWK: Having automorphisms weakens key, Cryptology ePrint Archive, Paper 2025/928. Available at https://eprint.iacr.org/2025/928.

[32] Mureau G, Pellet-Mary A, Pliatsok G, Wallet A (2024) Cryptanalysis of rank-2 module-lip in totally real number fields. *Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2024* (Springer), pp 226–255. DOI:10.1007/978-3-031-58754-2_9

[33] Allombert B, Pellet-Mary A, van Woerden W (2025) Cryptanalysis of rank-2 module-lip: a single real embedding is all it takes. *Advances in Cryptology – EUROCRYPT 2025* (Springer), *LNCS*, Vol. 15602, pp 184–212. DOI:10.1007/978-3-031-91124-8_7. See also https://eprint.iacr.org/2025/280

[34] Baum C, Braun L, de Saint Guilhem CD, Kloo"s 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.

[35] Baum C, Braun L, de Saint Guilhem CD, Kloo"s 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. DOI:10.1007/978-3-031-38554-4_19

[36] Yang K, Sarkar P, Weng C, Wang X (2021) QuickSilver: Efficient and affordable zero-knowledge proofs for circuits and polynomials over any field, Cryptology ePrint Archive, Paper 2021/076. DOI:10.1145/3460120.3484556. Available at https://eprint.iacr.org/2021/076

[37] Roy L (2022) SoftSpokenOT: Quieter OT extension from small-field silent VOLE in the minicrypt model, Cryptology ePrint Archive, Paper 2022/192. DOI:10.1007/978-3-031-15802-5_23. Available at https://eprint.iacr.org/2022/192

[38] Feneuil T (2024) The Polynomial-IOP Vision of the Latest MPCitH Frameworks for Signature Schemes, Post-Quantum Algebraic Cryptography - Workshop 2. Available at https://www.thibauld-feneuil.fr/docs/talks/2024-11-08_IHP-PQC_piop-based-sigs.pdf.

[39] Baum C, Beullens W, Mukherjee S, Orsini E, Ramacher S, Rechberger C, Roy L, Scholl P (2024) One tree to rule them all: Optimizing GGM trees and OWFs for post-quantum signatures, Cryptology ePrint Archive, Paper 2024/490. DOI:10.1007/978-981-96-0875-1_15. Available at https://eprint.iacr.org/2024/490

[40] Baum C, Beullens W, Braun L, de Saint Guilhem CD, Klooß M, Majenz C, Mukherjee S, Orsini E, Ramacher S, Rechberger C, Roy L, Scholl P (2026) Shorter, tighter, FAESTer: Optimizations and improved (QROM) analysis for VOLE-in-the-head signatures, Cryptology ePrint Archive, Paper 2026/164. Available at https://eprint.iacr.org/2026/164.

[41] Baum C, Beullens W, Braun L, de Saint Guilhem CD, Klooß M, Majenz C, Mukherjee S, Orsini E, Ramacher S, Rechberger C, Roy L, Scholl P (2025) Shorter, tighter, faester: Optimizations and improved (QROM) analysis for vole-in-the-head signatures. *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part VI*, eds Kalai YT, Kamara SF (Springer), *Lecture Notes in Computer Science*, Vol. 16005, pp 124–156. DOI:10.1007/978-3-032-01887-8_5. See also https://eprint.iacr.org/2026/164. Available at https://doi.org/10.1007/978-3-032-01887-8_5

[42] Jendral S, Dubrova E (2025) Side-channel and fault injection attacks on VOLEitH signature schemes: A case study of masked FAEST, Cryptology ePrint Archive, Paper 2025/378. DOI:10.46586/tches.v2026.i1.225-249. Available at https://eprint.iacr.org/2025/378

[43] Adj G, Aragon N, Barbero S, Bardet M, Bellini E, Bidoux L, Chi-Domínguez JJ, Dyseryn V, Esser A, Feneuil T, Gaborit P, Neveu R, Rivain M, Rivera-Zamarripa L, Sanna C, Tillich JP, Verbel J, Zweydinger F (2025) Mirath Signature Scheme. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mirath-spec-round2-web.pdf.

[44] 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.

[45] 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.

[46] Bidoux L, Feneuil T, Gaborit P, Neveu R, Rivain M (2024) Dual support decomposition in the head: Shorter signatures from rank sd and minrank. *International Conference on the Theory and Application of Cryptology and Information Security* (Springer), pp 38–69. DOI:10.1007/978-981-96-0888-1_2

[47] D'Alconzo G, Esser A, Gangemi A, Sanna C (2024) Sneaking up the ranks: Partial key exposure attacks on rank-based schemes, Cryptology ePrint Archive, Paper 2024/1628. Available at https://ia.cr/2024/1628.

[48] Kosuge H, Xagawa K (2025) New security proofs of MPC-in-the-head signatures in the quantum random oracle model, Cryptology ePrint Archive, Paper 2025/1999. Available at https://eprint.iacr.org/2025/1999.

[49] Adj G, Aragon N, Barbero S, Bardet M, Bellini E, Bidoux L, Chi-Domínguez JJ, Dyseryn V, Esser A, Feneuil T, Gaborit P, Neveu R, Rivain M, Rivera-Zamarripa L, Sanna C, Tillich JP, Verbel J, Zweydinger F (2025) Mirath signature scheme, . Version 2.1.0 Available at https://pqc-mirath.org/assets/downloads/mirath_v2.1.0.pdf.

[50] Benadjila R, Bouillaguet C, Feneuil T, Rivain M (2025) Algorithm Specifications and Supporting Documentation (Version 2.0). Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mqom-spec-round2.pdf.

[51] Feneuil T, Rivain M (2025) Threshold computation in the head: Improved framework for post-quantum signatures and zero-knowledge arguments. *Journal of Cryptology* 38(3):28. See also https://eprint.iacr.org/2023/1573.

[52] Feneuil T, Rivain M (2026) On the security of MPC-in-the-head signatures with correlated GGM trees, Cryptology ePrint Archive, Paper 2026/615. Available at https://eprint.iacr.org/2026/615.

[53] Kosuge H, Xagawa K (2026) Towards formal security proofs of MQOM, Cryptology ePrint Archive, Paper 2026/629. Available at https://eprint.iacr.org/2026/629.

[54] Aaraj N, Bettaieb S, Bidoux L, Budroni A, Dyseryn V, Esser A, Feneuil T, Gaborit P, Kulkarni M, Mateu V, Palumbi M, Perin L, Rivain M, Tillich JP, Xagawa K (2025) PERK, version 2.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/perk-spec-round2-web.pdf.

[55] Bettaieb S, Bidoux L, Gaborit P, Kulkarni M (2024) Modelings for generic PoK and applications: Shorter SD and PKP based signatures, Cryptology ePrint Archive, Paper 2024/1668. Available at https://eprint.iacr.org/2024/1668.

[56] Budroni A, Defranceschi M, Pintore F (2025) Recursion enabled: Improved cryptanalysis of the permuted kernel problem, Cryptology ePrint Archive, Paper 2025/2073. Available at https://eprint.iacr.org/2025/2073.

[57] Aragon N, Bardet M, Bidoux L, Chi-Domınguez JJ, Dyseryn V, Feneuil T, Gaborit P, Joux A, Neveu R, Rivain M, Tillich J, Vincotte A (2025) RYDE Signature Scheme. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/ryde-spec-round2-web.pdf.

[58] Aragon N, Bardet M, Bidoux L, Chi-Domınguez JJ, Dyseryn V, Feneuil T, Gaborit P, Joux A, Neveu R, Rivain M, Tillich J, Vincotte A (2025) RYDE v2.1 Release.

Available at https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/jkooTbyNBMw/m/gGjd9yZIAAAJ.

[59] Melchor CA, Bettaieb S, Bidoux L, Feneuil T, Gaborit P, Gama N, Gueron S, Howe J, Hülsing A, Joseph D, Joux A, Kulkarni M, Persichetti E, Randrianarisoa TH, Rivain M, Yue D (2025) The Syndrome Decoding in the Head (SD-in-the-Head) Signature Scheme, Algorithm Specifications and Supporting Documentation – Version 2.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/sdith-spec-round2-web.pdf.

[60] Ouyang Y, Tang D, Xu Y (2024) Code-based zero-knowledge from vole-in-the-head and their applications: simpler, faster, and smaller. *International Conference on the Theory and Application of Cryptology and Information Security* (Springer), pp 436–470. See also https://eprint.iacr.org/2024/1414.

[61] Esser A, Bellini E (2022) Syndrome decoding estimator. *IACR International Conference on Public-Key Cryptography* (Springer), pp 112–141. DOI:10.1007/978-3-030-97121-2_5

[62] Beullens W, Chen MS, Ding J, Gong B, Kannwischer MJ, Patarin J, Peng BY, Schmidt D, Shih CJ, Tao C, Yang BY (2025) UOV: Unbalanced Oil and Vinegar, Algorithm Specifications and Supporting Documentation, Version 2.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/uov-spec-round2-web.pdf.

[63] Jin Y, Pan Y, He X, Gong B, Ding J (2025) Security analysis on UOV families with odd characteristics: Using symmetric algebra, Cryptology ePrint Archive, Paper 2025/1137. Available at https://eprint.iacr.org/2025/1137.

[64] Beullens W, Campos F, Celi S, Hess B, Kannwischer MJ (2025) MAYO, Round 2 Version. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mayo-spec-round2.pdf.

[65] Furue H, Ikematsu Y, Hoshino F, Takagi T, Kosuge H, Yamakoshi K, Akiyama R, Nakamura S, Orihara S, Kinjo K (2025) QR-UOV. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/qruov-spec-round2-web.pdf.

[66] 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. DOI:10.1007/978-3-030-92068-5_7

[67] Amagasa H, Ueno R, Homma N (2025) AVX2 implementation of QR-UOV for modern x86 processors, Cryptology ePrint Archive, Paper 2025/1599. Available at https://eprint.iacr.org/2025/1599.

[68] May A, Ostuzzi M, Ressler H (2025) Just guess: Improved (quantum) algorithm for the underdetermined MQ problem, Cryptology ePrint Archive, Paper 2025/1788. Available at https://eprint.iacr.org/2025/1788.

[69] Wang LC, Chou CY, Ding J, Kuan YL, Leegwater JA, Li MS, Tseng BS, Tseng PE, Wang CC (2025) SNOVA Proposal for NISTPQC: Additional Digital Signature Schemes, Version 2.0. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2.pdf.

[70] Beullens W (2025) Improved cryptanalysis of SNOVA. *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VI*, eds Fehr S, Fouque P (Springer), *Lecture Notes in Computer Science*, Vol. 15606, pp 277–293. DOI:10.1007/978-3-031-91095-1_10. Available at https://doi.org/10.1007/978-3-031-91095-1_10

[71] 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. DOI:10.1145/3659467.3659900

[72] 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. DOI:10.1007/978-3-031-62746-0_4

[73] Wang LC, Chou CY, Ding J, Kuan YL, Leegwater JA, Li MS, Tseng BS, Tseng PE, Wang CC (2025) Round 2 SNOVA update, 6th PQC Standardization Conference, held September 24-26, 2025, in Gaithersburg, MD, USA. Available at https://csrc.nist.gov/csrc/media/presentations/2025/snova/images-media/snova-tseng_1.5.pdf.

[74] Ding J, Guo H, Kuan YL, Leegwater JA, Li P, Tseng PE, Wang LC (2026) Reformulating the SNOVA signature scheme, Cryptology ePrint Archive, Paper 2026/659. Available at https://eprint.iacr.org/2026/659.

[75] (2024) NIST pqc-forum mailing list. Available at https://groups.google.com/a/list.nist.gov/g/pqc-forum.

Appendix A List of Abbreviations and Acronyms

AES: Advanced Encryption Standard

DNSSEC: Domain Name System Security Extensions

DSS: Digital Signature Standard

EUF-CMA: Existentially Unforgeable against Chosen Message Attacks

FIPS: Federal Information Processing Standards

IKE: Internet Key Exchange

IPsec: Internet Protocol Security

ITL: Information Technology Laboratory

KEM: Key Encapsulation Mechanism

LCE: Linear Code Equivalence

MPC: Multi-Party Computation

MPCitH: Multi-Party Computation in the Head

MQ: Multivariate Quadratic

NIST: National Institute of Standards and Technology

NIST IR: NIST Internal Report

OCSP: Online Certificate Status Protocol

OT: Oblivious Transfer

PIOP: Polynomial Interactive Oracle Proof

PKP: Permuted Kernel Problem

PQC: Post-Quantum Cryptography

PRG: Pseudorandom Generator

QROM: Quantum Random Oracle Model

RAM: Random-Access Memory

ROM: Random Oracle Model

RREF: Reduced Row Echelon Form

RSD: Restricted Syndrome Decoding

SD: Syndrome Decoding

SP: Special Publication

SSH: Secure Shell

SUF-CMA: Strong Unforgeability against Chosen Message Attacks

TCitH: Threshold Computation in the Head

TLS: Transport Layer Security

VOLEitH: Vector Oblivious Linear Evaluation in the Head

ZKPoK: Zero-Knowledge Proof of Knowledge