NISTIR 8309

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Jacob Alperin-Sheriff
Daniel Apon
David Cooper
Quynh Dang
John Kelsey
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8309

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8309

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Jacob Alperin-Sheriff*
Daniel Apon
David Cooper
Quynh Dang
John Kelsey
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone
Computer Security Division
Information Technology Laboratory

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

**Former employee; all work for this publication was done while at NIST*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8309

July 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8309
39 pages (July 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8309

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: pqc-comments@nist.gov

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.

Abstract

The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public, competition-like process. The new public-key cryptography standards will specify one or more additional digital signatures, public-key encryption, and key-establishment algorithms to augment Federal Information Processing Standard (FIPS) 186-4, *Digital Signature Standard (DSS)*, as well as NIST Special Publication (SP) 800-56A Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, and SP 800-56B Revision 2, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

The NIST Post-Quantum Cryptography Standardization Process began in 2017 with 69 candidate algorithms that met both the minimum acceptance criteria and submission requirements. The first round lasted until January 2019, during which candidate algorithms were evaluated based on their security, performance, and other characteristics. NIST selected 26 algorithms to advance to the second round for more analysis. This report describes the evaluation and selection process, based on public feedback and internal review, of the second-round candidates. The report summarizes the 26 second-round candidate algorithms and identifies those selected to move forward to the third round of the competition. The third-round finalist public-key encryption and key-establishment algorithms are Classic McEliece, CRYSTALS-KYBER, NTRU, and SABER. The third-round finalists for digital signatures are CRYSTALS-DILITHIUM, FALCON, and Rainbow. These finalists will be considered for standardization at the end of the third round. In addition, eight alternate candidate algorithms will also advance to the third round: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic, and SPHINCS+. These additional candidates are still being considered for standardization, although this is unlikely to occur at the end of the third round. NIST hopes that the announcement of these finalists and additional candidates will serve to focus the cryptographic community's attention during the next round.

Keywords

cryptography; digital signatures; key-establishment mechanism (KEM); post-quantum cryptography; public-key encryption; quantum resistant; quantum safe.

Supplemental Content

The NIST Post-Quantum Cryptography Standardization Process webpage is available at:

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Acknowledgments

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

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 and second rounds. NIST would not be able to select new post-quantum public-key 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 Post-Quantum Cryptography 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 Larry Bassham, Lily Chen, Thinh Dang, Morris Dworkin, Sara Kerman, and Andrew Regenscheid.

Table of Contents

1 Introduction

In recent years, there has been steady progress in building quantum computers. If large-scale quantum computers are realized, they would threaten the security of many commonly-used public-key cryptosystems. Key-establishment schemes and digital signatures based on factoring, discrete logarithms, and elliptic curve cryptography will be the most severely affected. (Symmetric cryptographic primitives, such as block ciphers and hash functions, will only be mildly affected.) In response, there has been intense research into post-quantum cryptography. This science is the study of cryptosystems that would be secure against adversaries who have both quantum and classical computers and that can be deployed without drastic changes to existing communication networks and protocols.

Motivated by these considerations, the National Institute of Standards and Technology (NIST) is in the process of selecting public-key cryptographic algorithms through a public, competition-like process. The new public-key cryptography standards will specify one or more additional algorithms for digital signatures, public-key encryption, and key-establishment. The new standards will augment Federal Information Processing Standard (FIPS) 186-4, *Digital Signature Standard (DSS)* [1], as well as Special Publication (SP) 800-56A Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [2], and SP 800-56B Revision 2, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography* [3]. It is intended that these algorithms will be capable of protecting sensitive U.S. Government information well into the foreseeable future, including after the advent of quantum computers. The competition-like process will be referred to as the NIST Post-Quantum Cryptography (PQC) Standardization Process hereafter in this document.

The NIST PQC Standardization Process began in December 2016, when NIST issued a public call for submissions of post-quantum public-key cryptographic algorithms [4]. A total of 82 candidates were submitted by the November 2017 deadline. In December 2017, NIST announced that 69 of these candidates met both the submission requirements and the minimum acceptability criteria and were accepted into the first round of the standardization process. Submission packages for the first-round candidates were posted online at https://www.nist.gov/pqcrypto for public review and comment.

In January 2019, based on public feedback and internal reviews of the candidates, NIST selected 26 algorithms to move on to the second round of the standardization process [5]. These algorithms were viewed as the most promising candidates for eventual standardization. During the second round, these candidates were subjected to more detailed analysis by NIST and the broader cryptographic community. This analysis included more thorough checking of the theoretical and empirical evidence used to justify the security of these cryptosystems, more careful benchmarking of the performance of these algorithms using optimized implementations on a variety of hardware platforms and under realistic conditions, and consideration of other factors that could aid or hinder the practical deployment of these cryptosystems.

The second round began on January 30, 2019, and continued until July 22, 2020. The Second NIST PQC Standardization Conference was held in Santa Barbara, CA on August 22-24, 2019, co-located with the CRYPTO 2019 conference. Each submission team was invited to present an update on their candidate algorithm. In addition, several researchers presented work that was

relevant to the PQC standardization process. NIST also held an open discussion session to gather input from attendees. As in the first round, NIST received much feedback from the cryptographic community.

After careful deliberation and analysis, NIST has selected seven finalists and eight alternates to move on to the third round. NIST intends to select a small number of the finalists for standardization at the end of the third round. In addition, NIST expects to standardize a small number of the alternate candidates (most likely at a later date).

Below is a timeline of major events with respect to the NIST PQC Standardization Process to date.

Table 1: NIST PQC Standardization Process Timeline

April 2-3, 2015	Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg, MD
February 24, 2016	PQC Standardization: Announcement and outline of NIST's Call for Submissions presentation given at PQCrypto 2016 [5]
April 28, 2016	NISTIR 8105, *Report on Post-Quantum Cryptography*, released [6]
December 20, 2016	Federal Register Notice – Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [7]
November 30, 2017	Submission Deadline for NIST PQC Standardization Process
December 20, 2017	First-round candidates announced. The public comment period on the first-round candidates began.
April 11-13, 2018	First NIST PQC Standardization Conference, Ft. Lauderdale, FL [8]
January 30, 2019	Second-round candidates announced. NISTIR 8240, *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process* [9], released. The public comment period on the second-round candidates began.
April 1, 2019	Deadline for updated submission packages for the second round
August 22-24, 2019	Second NIST PQC Standardization Conference, Santa Barbara, CA
April 15, 2020	NIST invited comments from submitters and the community to inform its decision-making process for the selection of third-round candidates.
July 22, 2020	Third round finalists and alternate candidates announced. The public comment period on the third round began. NISTIR 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, released.

1.1 Purpose and Organization of this Document

The purpose of this document is to report on the second round of the NIST PQC Standardization Process. The report is organized as follows.

Section 2 enumerates the candidates that were included in the second round. A description of the evaluation criteria and selection process used to ultimately select the third-round finalists and alternate candidates is then provided. The third-round finalists and alternates are named.

Section 3 summarizes each of the second-round candidates. For each candidate, there is a brief description of the algorithm and its strengths, as well as characteristics that might be disadvantageous. This report presents reasons why candidate algorithms were selected or not selected for the third round.

Section 4 describes the next steps in the NIST PQC Standardization Process and the evaluation process for selecting algorithms that will be standardized.

2 Evaluation Criteria and the Selection Process

2.1 Acceptance of the Second-Round Candidates

NIST selected 26 candidate algorithms for the second round. Of the 26 candidates, 17 were key-establishment mechanisms (KEMs) or public-key encryption schemes, while nine were digital signatures. Submission teams were allowed to make minor modifications and re-submit their packages, which had to meet the same requirements as the original submissions. Four of the candidates were mergers of first-round algorithms: LEDAcrypt (merged from LEDAkem and LEDApkc), NTRU (merged from NTUEncrypt and NTRU-HRSS-KEM), ROLLO (merged from LAKE, LOCKER, and Ouroboros-R), and Round5 (merged from Hila5 and Round2). The complete updated specifications were posted on www.nist.gov/pqcrypto on April 10, 2019, for public review.

Table 2: Second-Round Candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

2.2 Evaluation Criteria

NIST's Call for Proposals [10] identified three broad aspects of the evaluation criteria that would be used to compare candidate algorithms throughout the NIST PQC Standardization Process: 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. These criteria are described below, along with a discussion of how they impacted the second-round candidate evaluations.

2.2.1 Security

As was the case for the past Advanced Encryption Standard (AES) and Secure Hash Algorithm 3 (SHA-3) competitions, security is the most important factor when evaluating the candidate post-quantum algorithms. NIST's current public-key standards are used in a wide variety of applications, including internet protocols like TLS, SSH, IKE, IPsec, and DNSSEC, as well as for certificates, software code signing, and secure bootloaders. New standards are needed to provide security for all of these applications.

For the purpose of quantifying the security of candidate algorithms, NIST gave three possible security definitions—two for encryption and one for signatures. NIST also designated five security strength categories for classifying the computational complexity of attacks that violate the security definitions (see [10]).

For general-use encryption and key-establishment schemes, the Call for Proposals [10] asked for "semantically secure" schemes with respect to adaptive chosen ciphertext attack (equivalently IND-CCA2 security[1]). For ephemeral use cases, NIST also accepted algorithms that provided semantic security with respect to chosen plaintext attack (IND-CPA security) since IND-CCA2 security is not required in strictly ephemeral use cases, and attempting to meet the more stringent requirements of IND-CCA2 security may incur significant performance penalties for some schemes. Digital signature schemes were required to provide existentially unforgeable signatures with respect to an adaptive chosen message attack (EUF-CMA security). Submitters were encouraged but not required to provide proofs of security in relevant models.

The five security strength categories defined in [10] were based on the computational resources required to perform certain brute force attacks against the existing NIST standards for AES and SHA in a variety of different models of the cost of computation, both classical and quantum. Submitters were asked to provide a preliminary classification of all proposed parameter sets according to these definitions. While category 1, 2, and 3 parameters were (and continue to be) the most important targets for NIST's evaluation, NIST nevertheless strongly encourages the submitters to provide at least one parameter set that meets category 5. Most of the candidate algorithms have already done this; a few have not.

NIST also mentioned other desirable security properties, such as perfect forward secrecy, resistance to side-channel and multi-key attacks, and resistance to misuse, all of which continue to be of interest. In addition, NIST required submission packages to summarize known cryptanalytic attacks on the scheme and complexity estimates for these attacks.

During the first and second rounds of the NIST standardization process, a number of cryptanalytic results dramatically reduced the security of some submitted schemes and undermined NIST's confidence in the maturity of others. These results were the basis for many of NIST's decisions thus far in the process.

As NIST moves closer to making standardization decisions, cryptanalysis aiming to precisely measures the security of various submitted parameter sets with respect to known attacks will become even more relevant. This may include, for example, precise quantification of decryption failure rates for CCA parameter sets, quantification of the concrete algorithmic complexity of lattice reduction, and designing and testing countermeasures to advanced side-channel attacks like differential power analysis. It would also be useful for researchers to use techniques from formal verification to ensure the correctness of security proofs. All of this work is important to provide the high degree of confidence necessary for NIST to standardize some of these schemes in the near future.

NIST also sees diversity of computational hardness assumptions as an important long-term security goal for its standards. NIST hopes to standardize practically efficient schemes from different families of cryptosystems to reduce the risk that a single breakthrough in cryptanalysis will leave the world without a viable standard for either key-establishment or digital signatures. Nonetheless, NIST does not feel the need to choose these standards all at once but will rather

[1] For the remainder of this document, IND-CCA2 security will simply be referred to as CCA security.

prioritize those schemes which seem closest to being ready for standardization and wide adoption. NIST feels this strategy best serves to balance the desire for diversity with the need for all standards to be thoroughly vetted before they are released.

2.2.2 Cost and Performance

The original call for proposals [10] identified cost as the *second* most important criterion when evaluating candidate algorithms. Cost includes the computational efficiency of key generation and public and private key operations, the transmission costs for public keys and signatures or ciphertexts, and the implementation costs in terms of RAM (random-access memory) or gate counts.

During the second round of the NIST PQC Standardization Process, more information about the computational efficiency of the algorithms became available. Faster, constant-time implementations on Intel x64 processors were provided for many of the algorithms, as were ARM Cortex-M4 and hardware implementations. These new implementations provided better information not only about the performance of the different algorithms but also about the resources required by implementations (RAM or gate counts). NIST hopes to see more and better data for performance in the third round. This performance data will hopefully include implementations that protect against side-channel attacks, such as timing attacks, power monitoring attacks, fault attacks, etc.

When comparing the overall performance of the algorithms, both computational cost and data transfer cost were considered. For this purpose, the algorithms were generally compared with respect to the two separate categories, leaving open the possibility that different algorithms will eventually be standardized for these two categories of use cases.

For general-purpose use, the evaluation of overall performance considered the cost of transferring the public key in addition to the signature or ciphertext during each transaction. For KEMs, algorithms that provided better overall performance when the cost of key generation was taken into account were preferred since many applications use a new KEM key pair for each transaction to provide forward secrecy. For signature algorithms, the cost of key generation was considered less important.

For special-purpose uses, the performance requirements can be somewhat different, and different algorithms may be preferable. For example, a few of the candidate algorithms are computationally efficient and have very small signatures or ciphertexts but very large public keys. While these algorithms may not provide the best overall performance when the public key needs to be sent for each connection, there are applications for which the public key is distributed in advance (e.g., as part of the software package) so that the cost of transmitting the public key is not part of the transaction cost. Algorithms with large public keys may work well with these applications even if they do not provide the best performance for other applications.

2.2.3 Algorithm and Implementation Characteristics

While current implementations of the candidate algorithms tend to run in constant time, there can be subtle issues which can be overlooked (see, for example, [11]). Most implementations do not provide protection against other types of side-channel attacks, such as power analysis. During the

third round, NIST hopes to collect more information about the costs of implementing these algorithms in a way that provides resistance to such attacks. Implementations on very constrained devices, such as smart cards, tend to be more vulnerable to such attacks than implementations on general-purpose computers since constrained devices are more likely to be used in environments in which the attacker has unrestricted access to the device. So, in addition to the cost in terms of computation time, the cost of implementing these mitigations in terms of RAM (or gate count) is also very important.

In addition, NIST has examined the potential performance impact of candidate algorithms in existing widely used protocols (e.g., TLS, IPSec, and SSH) and certificates. It is clear that some algorithms would cause major performance problems if dropped into those protocols—particularly schemes with very large public keys, ciphertexts, or signatures. Using these algorithms in such widely used protocols would require considerable re-engineering to achieve adequate performance. Other candidate algorithms could be substituted for existing signature and key establishment algorithms with a relatively small performance loss.

Several of the candidates made updates during the first and second rounds to improve simplicity. When considering standardization, simple and elegant designs are preferable, as they encourage further analysis and understanding. NIST will continue to pay close attention to how well-analyzed and well-understood candidates are during the third round.

As stated in [10], NIST will consider any factors which might hinder or promote the adoption of an algorithm or implementation, including but not limited to intellectual property covering an algorithm or its implementations and the availability and terms of licenses to interested parties. Considerations involving intellectual property may play a stronger role in the third round as NIST makes decisions regarding standardization. NIST has a clear preference for royalty-free algorithms in order to enable widespread adoption.

2.3 Selection of the Third-Round Finalists and Alternate Candidates

As mentioned in Section 2.2.1, a number of cryptanalytic results announced during the second round dramatically reduced the security of some submitted schemes and undermined NIST's confidence in the maturity of others. These results led to the elimination of some of the candidates from further consideration.

Of the remaining schemes, the second round provided NIST with a number of KEMs that could be standardized in the near future—many with similar designs, based on similar security assumptions, and with comparable performance. NIST is unlikely to standardize two or more very similar KEM algorithms, so some very strong candidates had to be eliminated in this round in order to focus analytical attention on the most promising ones. This was particularly the case for the structured lattice-based KEMs. By contrast, NIST had far fewer candidate signature algorithms to choose from at the end of the second round.

When choosing between very similar KEM algorithms, cost and performance were significant selection criteria. As noted in Section 2.2.2, when comparing candidates, both data transmission costs and computational efficiency were taken into account. NIST considered benchmarks

provided by the community (see, for example, [12, 13, 14, 15, 16]) across multiple platforms when determining computational efficiency.

NIST selected 15 of the second-round candidates to move onto the third round of the standardization process. Of the 15 advancing candidates, seven have been selected as finalists and eight as alternate candidates.

Table 3: Third-Round Finalists

Public-Key Encryption/KEMs	Digital Signatures
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

Table 4: Alternate Candidates

Public-Key Encryption/KEMs	Digital Signatures
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

The set of finalists are algorithms that NIST considers to be the most promising to fit the majority of use cases and most likely to be ready for standardization soon after the end of the third round. As CRYSTALS-KYBER, NTRU, and SABER are all structured lattice schemes, NIST intends to select, at most, one for the standard. The same is true for the signature schemes CRYSTALS-DILITHIUM and FALCON. In NIST's current view, these structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes.

The alternate candidates are regarded as potential candidates for future standardization, most likely after another round of evaluation. Some of the alternate candidates have worse performance than the finalists but might be selected for standardization based on NIST's high confidence in their security. Others have acceptable performance but require additional analysis or other work to inspire sufficient confidence in their security for NIST to standardize. In addition, some alternate candidates were selected based either on NIST's desire for diversity in future post-quantum security standards or on their potential for further improvement.
During the third round, the term "finalist" will refer to the first seven algorithms listed above, and the terms "alternate" or "alternate candidate" will be used for the other eight algorithms also advancing.

3 Summary of Second-Round Candidates

Each of the second-round candidates is discussed below, including a summary of their advantages and disadvantages. In addition, the discussion provides reasons why a scheme was (or was not) selected to advance to the third round. Some suggestions are included that the submitters of advancing schemes may wish to address for the third round.

The 17 public-key encryption and key-establishment schemes are discussed first (in Sections 3.1 to 3.17), and the nine digital signature schemes follow (in Sections 3.18 to 3.26). The finalists are presented first, followed by the alternate candidates and then the algorithms not selected to advance to the third round.

3.1 Classic McEliece (merger of Classic McEliece and NTS-KEM)

Classic McEliece is a code-based KEM based on the 1979 McEliece cryptosystem built from a hidden Goppa code. Classic McEliece includes some modern improvements for efficiency and to provide CCA security. The security of these improvements is reduced to the one-wayness against chosen-plaintext attack (OW-CPA) security of the original construction as proposed in 1979 [17]. The original construction is not based on a particularly natural computational assumption; however, Goppa code McEliece and related cryptosystems have a long history of study.

Classic McEliece has a somewhat unusual performance profile—it has a very large public key but the smallest ciphertexts of all competing KEMs. This is not a good fit for general use in internet protocols as they are currently specified, but in some applications, the very small ciphertext size could make Classic McEliece an appealing choice (for example, see [18]).

Goppa code McEliece has been a well-known construction for over 40 years with only incremental improvements on attacks. Due to the confidence this fact inspires in the construction, as well as the careful implementation work of the submitters, Classic McEliece has a stable specification––the only significant change in the second round is the addition of additional parameter sets. As such, NIST selected Classic McEliece as a finalist and believes it could be ready for standardization (should NIST choose to select it) at the end of the third round.

3.2 CRYSTALS-KYBER

CRYSTALS-KYBER is a KEM whose security is based on the presumed hardness of the Module Learning With Errors (MLWE) problem. At its core is Regev's original idea for public-key encryption from plain LWE [19]. CCA security is achieved with a Fujisaki-Okamoto transform [20, 21] and is supported by a security proof in the quantum random oracle model (QROM). While MLWE is a relatively young problem, no attacks are known against MLWE that do not also apply to the more well-established plain LWE. The module structure of KYBER is over a power-of-two cyclotomic ring, enabling fast computations via the number theoretic transform (NTT). The scheme has excellent all-around performance for most applications. It also enables relatively straightforward adjustment of the performance/security trade-off by varying module rank and noise parameters. In addition, CRYSTALS-KYBER shares a common framework with the CRYSTALS-DILITHIUM signature scheme, which is also a finalist.

For Round 2, KYBER no longer uses the public-key compression that was present in the first-round version. The modulus and noise parameters were also adjusted. Final key derivation now uses SHAKE256 instead of SHA3-256. During the second round, a new fault attack forcing nonce reuse was discovered, affecting several lattice schemes, including KYBER [22]. Recent theoretical work has placed MLWE on stronger footing by providing a very tight reduction from ring LWE to module LWE [23].

Compared to other lattice schemes, KYBER has relatively lower "CoreSVP" [24] security strength when targeting security strength category 1. NIST believes it is important to understand how exactly this CoreSVP security translates into "true" bit security strength for KYBER. KYBER's performance in side-channel-resistant implementations will be closely considered by NIST in the third round. NIST views CRYTALS-KYBER as one of the most promising KEM schemes to be considered for standardization at the end of the third round.

3.3 NTRU

NTRU is a structured lattice-based KEM whose security is based on a different assumption than the Ring-LWE (RLWE) or MLWE-based approach of several of the other lattice-based candidates. Although it lacks a formal worst-case-to-average-case reduction, NTRU has a long and established history and is a very widely analyzed scheme. Versions of NTRU have also been standardized by other organizations [25, 26]. In Round 2, the NTRU submission was the result of a merger of the NTRUEncrypt and NTRU-HRSS-KEM first-round submissions. This variant of NTRU under consideration satisfies perfect correctness and uses an improved CCA transform with a security proof in the QROM. While NTRU is very efficient, it is not quite at the level of the highest-performing lattice schemes. In particular, NTRU has slower key generation than the schemes based on RLWE and MLWE.

NTRU provided two different cost models for estimating the security of its parameter sets: a local and a non-local model. The non-local model is most similar to the CoreSVP metric used by the other lattice-based submissions, and in this model, the NTRU submission lacks a category 5 parameter set proposal. Likewise, the lowest security parameter set in the NTRU submission (ntruhps2048509) does not meet security category 1, according to the non-local model. NTRU also proposed a more aggressive local model, which assigns higher security to the parameter sets. If NTRU's parameter sets are treated as targeting the security categories assigned by the local model, then they would have lower CoreSVP complexity than many of the other schemes targeting the same security strength categories. It is important to understand exactly how these various cost metrics translate into "true" bit security strengths.

NIST sees structured lattice-based schemes as very promising. As NTRU is such a scheme but based on a different security assumption than RLWE or MLWE, it provides some diversity to the collection of finalists. While NTRU has a small performance gap in comparison to KYBER and SABER, its longer history was an important factor in NIST's decision to select NTRU as a finalist. Due to its longer history, NTRU has less risk of unexpected intellectual property claims.

NIST expects that, at most, only one of these candidates—KYBER, SABER, or NTRU—will be standardized at the end of the third round. In the event that new cryptanalytic or intellectual

property issues threaten the future of KYBER and SABER, NTRU would be seen as a more appealing finalist.

3.4 SABER

SABER is a KEM whose security is based on the presumed hardness of the Module Learning With Rounding (MLWR) problem, a variant of MLWE where the addition of small error terms is replaced by rounding from one modulus to a smaller, second modulus. CCA security is given by a variant of the Fujisaki-Okamoto transform. While reductions to MLWR from MLWE exist, they are not concretely applicable to SABER, which is a mild concern. It should be noted that reductions exist from MLWE to a shortest vector problem, but they are also not concretely applicable to the MLWE candidates, such as KYBER. On the other hand, the rounding operation and power-of-2 moduli in SABER allow for the efficient optimization of the modular reduction and polynomial multiplication steps. Overall, SABER has excellent performance and would be immediately suitable for general-purpose applications.

A few minor changes were made in SABER's specification for the second round. Notably, a small tweak allowed for a successful formal reduction from the security of SABER to Module-LWR.

NIST currently has no suggestions for changes to the SABER specification but believes that there are many valuable avenues for research in this area. In particular, NIST encourages additional research regarding side-channel analysis and optimization of the non-NTT style of multiplication that is unique to SABER among the lattice candidates, as well as on the concrete differences between the security of MLWE and MLWR for the proposed parameter sets. The performance of side-channel-resistant implementations of SABER will be closely considered by NIST during the third round. As mentioned above, SABER is one of the most promising KEM schemes to be considered for standardization at the end of the third round.

3.5 BIKE

BIKE is a structured code-based KEM which offers balanced performance for general use, similar to structured lattice-based KEMs but with somewhat slower decapsulation and key generation and somewhat more bandwidth (public-key size plus ciphertext size). This performance profile, which optimizes bandwidth for BIKE, was chosen by the submitters at the end of the second round from three different performance profiles offered in BIKE's initial second-round submission. A new decoder was also introduced during the second round and is detailed below.

The most significant attacks for both passive key recovery and message recovery for BIKE are based on information-set decoding, and complexity estimates for this family of attacks have been much more stable than for most other classes of attacks. As such, a scheme like BIKE would, if standardized, provide a useful fallback in the case of major cryptanalytic advances against structured lattice schemes.

Nonetheless, there remain serious questions about side-channel protections and CCA security that need to be resolved before BIKE can be considered for standardization. BIKE pays a significant performance penalty by targeting CCA security since a very low decapsulation failure

rate is required. The decapsulation failure rate is estimated in a heuristic way by using simplified models to extrapolate from experiments [27]. The submitters announced a redesign of the decoder (switching from a backflip decoder to a Black-Gray-Flip [BGF] decoder [28]) and altered their parameters at the end of the second round to better meet their target decapsulation failure rate. As of the end of the second round, however, the submitters were not confident enough to explicitly claim CCA security.

Additionally, the BIKE submitters provided a new implementation designed to be constant time and without secret dependent memory access. As both the parameters and the implementation are quite new, both will require vetting by the community, in particular regarding side-channel protections and decapsulation failure rates. Finally, BIKE did not provide category 5 parameters in their most recent update. NIST strongly encourages that such parameters be added.

NIST views BIKE as one of the most promising code-based candidates. As mentioned above, more time will be needed to address the security concerns listed. As such, BIKE was not chosen to be a finalist but will advance to the third round for more study.

3.6 FrodoKEM

FrodoKEM is a KEM whose security is based on the presumed hardness of the plain LWE problem. Frodo is quite close to Regev's original LWE public-key encryption construction, together with a Fujisaki-Okamoto transform to reach CCA security, supported by a security proof in the QROM. Among lattice-based schemes, Frodo has the least amount of structure and is thus likely to be less susceptible to algebraic attacks. Plain LWE itself is among the most studied and analyzed cryptographic problems in existence today. The resulting potential security advantages of Frodo are paid for with far worse performance in all metrics than other lattice schemes. However, Frodo still has some performance advantages over other conservative options, particularly in key generation time and public-key size.

The Frodo team added a parameter set for security category 5 during the second round. Certain pseudorandomness expansion procedures were moved to the key generation function, apparently avoiding the aforementioned fault attack of [22]. In addition, the Fujisaki-Okamoto transform was somewhat simplified based on new theory results on QROM security. Also, during the second round, a new theoretical analysis of lattice algorithms "with hints" showed that certain power trace attacks against Frodo are stronger than previously believed [29].

Use of FrodoKEM would have a noticeable performance impact on high traffic TLS servers, where each server does decapsulation which requires close to 2 million cycles for the best performing parameter set (FrodoKEM-640-AES) and receives a public key and a ciphertext (around 20,000 bytes in total) for every fresh key exchange.

In NIST's view, FrodoKEM may be suitable for use cases where the high confidence in the security of unstructured lattice-based schemes is much more important than performance. NIST's first priority for standardization is a KEM that would have acceptable performance in widely used applications overall. As such, possible standardization for FrodoKEM can likely wait until after the third round. FrodoKEM could also serve as a conservative backup in the case of new cryptanalytic results targeting structured lattices being discovered in the third round. For these

reasons, FrodoKEM was not selected as a finalist but is one of the alternate candidates advancing.

3.7 HQC

HQC is a code-based KEM based on the hardness of the decisional quasi-cyclic syndrome decoding (QCSD) with parity problem. The scheme claims CCA2 security based on a rigorous analysis of its decryption failure rate.

In the second round, a new analysis of the error vector distribution showed that the decryption failure rate was lower than previously believed, allowing reductions in key sizes. The HQC team also presented a new decoder using concatenated Reed-Muller and Reed-Solomon codes, further reducing the size of the public keys. Even with these key size reductions, the resulting public keys and ciphertexts are 1.6-2 and 4-5 times the size of those of BIKE, respectively. Although the bandwidth of HQC exceeds that of BIKE, HQC's key generation and decapsulation functionalities are much faster than BIKE's.

During the third round, NIST encourages further research into the relationship between the decisional and search versions of the QCSD with parity problems as well as a close analysis of the new parameter sets. The community should also continue to investigate the effects on security produced by the quasi-cyclic code structure.

While HQC offers strong security assurances and a mature analysis, its performance characteristics are overshadowed by the structured lattice KEM candidates, and it compares unfavorably with BIKE in the bandwidth metric. As a result of these facts, NIST did not select HQC as a finalist for the first round of NIST standards. HQC is advancing as an alternate candidate in the third round due to the thoroughness of its security analysis in comparison to BIKE, the other strong code-based KEM candidate.

3.8 NTRU Prime

NTRU Prime is a collection of two lattice-based KEMs, Streamlined NTRU Prime and NTRU LPRime, which share many design elements but differ in algebraic structure. Streamlined NTRU Prime is an "NTRU-like" KEM with a quotient structure in its public key, and NTRU LPRime is an "RLWE-like" KEM with a product structure in its public key. Streamlined NTRU Prime is secure under an assumption similar to that made for classical NTRU, which is in turn based on a long and established history of resisting cryptanalysis. NTRU LPRime was designed with a structure chosen by analogy to RLWE schemes based on the work of Lyubashevsky, Peikert, and Regev [30].

Recent work on reduction-based security for lattice cryptography covers NTRU LPRime "in spirit" through the work of Peikert, Regev, and Stephens-Davidowitz [31]. NTRU Prime has no decryption failures and thus is immune to decryption failure boosting attacks. It achieves CCA security through a Fujisaki-Okamoto-type transform. The central distinction between NTRU Prime and other structured lattice KEM proposals is its abandonment of the cyclotomic ring structure in favor of the field $Z_q[x]/(x^p-x-1)$. This choice is partly motivated by recent progress in quantum algorithms for finding short vectors in principal ideal lattices with a guaranteed short generator.

In the second round, two new parameter sets were introduced. NTRUprime's parameter sets target security strength categories 2, 3, and 4. This results in a narrower range of CoreSVP values than other lattice submissions targeting security strengths 1, 3, and 5. NIST encourages NTRUprime to consider expanding the range of security strengths targeted by including category 5 parameter sets. Additionally, while NTRUprime's category 2 parameter sets at least have a higher CoreSVP value than most of the lattice schemes targeting category 1, the category 3 and 4 parameter sets are quite aggressive compared to most of the other submissions targeting the same security categories, and whether they actually meet their claimed security categories will need to be determined.

NTRU Prime was advanced to the third round but not as a finalist. Additional motivation for NTRU Prime's unique choice of algebraic structure could be gained by new progress in algebraic cryptanalysis of cyclotomic structures during the third round, provided that it undermines NIST's confidence in cyclotomic structures but clearly does not extend to NTRUprime's choice of $Z_q[x]/(x^p-x-1)$.

3.9 SIKE

SIKE is unique among the second-round candidates—it is the only scheme based on isogenies of elliptic curves. One of the main advantages to SIKE is that it has the smallest public key sizes of all of the encryption and KEM schemes, as well as very small ciphertext sizes. As part of their second-round update, the SIKE team introduced a version with even smaller (compressed) keys. The parameters are also easy to scale.

The status report on the first round [9] noted that the basic security problem upon which SIKE is based is an area where further study would be useful. Towards the end of the first round, a series of papers [32, 33] examined the relevant classical and black-box quantum attacks, resulting in confidence that existing parameter sets were providing more security than previously claimed. As a result, the SIKE team was able to lower the parameter sizes used in their second-round specification. One caveat regarding SIKE's analysis is that its assignment of security strength categories relies on the assumption that adversaries are limited to no more than 2^{96} bits of memory. While this may perhaps be a reasonable assumption when assigning parameter sets to security strength categories 1 and 2, considerations such as maximum achievable circuit depth suggest that adversaries with more memory should be considered when assigning parameter sets to categories 3 and above. Independent of this particular issue, NIST believes that confidence in the hardness of the SIDH (supersingular isogeny Diffie-Hellman) problem would continue to benefit from more study.

The main drawback to SIKE is that its performance (measured in clock cycles) is roughly an order of magnitude worse than many of its competitors. Much work has been done to optimize implementations, including the compressed-key version, and it is hoped that such optimizations continue. While some existing techniques for side-channel protection are known for computing multiples of points on elliptic curves, more research is also needed on protecting the isogeny computations.

NIST sees SIKE as a strong candidate for future standardization with continued improvements and accordingly selected SIKE to move into the third round as an alternate candidate. There are

applications which would benefit from SIKE's small key and ciphertext sizes and which may be able to accept the performance impact. Further research in isogeny-based cryptography is encouraged.

3.10 LAC

LAC is a KEM whose security is based on the hardness of the RLWE problem. LAC has an unusual design feature: it uses error-correcting codes to "fix" decryption failures. (This idea also appears in Round5.) This means that LAC can tolerate a higher decryption failure rate, which allows it to use a smaller modulus that leads to improved performance. However, care is needed to ensure that this design does not lead to security vulnerabilities. During the first round of the NIST standardization process, several authors published attacks on LAC that reduced its security to below the required levels [34, 35, 36, 37]. These included chosen-ciphertext attacks that worked by artificially increasing the decryption failure rate and side-channel attacks that exploit non-constant-time implementations of the error-correction procedures in LAC. LAC was subsequently modified to resist these attacks.

During the second round, a few more minor security issues were discovered, including another issue involving variable-time implementation of error-correction procedures. These issues were described in the public "official comments" during the first and second rounds of the NIST standardization process [38].

NIST is concerned that the cryptanalysis of LAC seems to involve precisely those aspects of LAC's design, particularly the use of error correction, that distinguish it from most other structured lattice-based schemes. Although LAC has been modified to resist those attacks, NIST believes that further study is needed before it can be confident that there are no remaining vulnerabilities in the LAC design. Thus, despite very good performance numbers, LAC was not selected to move on to the third round.

3.11 LEDAcrypt

LEDAcrypt includes structured code-based KEM and encryption schemes using a similar construction to BIKE. LEDAcrypt differs from BIKE in a few of its design decisions. In particular, LEDAcrypt designed its parameter sets to have more rigorously bounded decryption failure rates than BIKE. As a result, the parameters targeting CCA security have about 60 % larger bandwidth than BIKE.

In the first- and second-round submissions, the private key of LEDAcrypt had additional product structure relative to BIKE. As with BIKE, the private key consisted of a sparse quasi-cyclic matrix, but in the case of LEDAcrypt, this sparse quasi-cyclic matrix was produced by multiplying two sparser quasi-cyclic matrices. This additional structure enabled an attack [39] during the second round, which primarily consisted of a large class of weak keys where a modified information set decoding results in a much more efficient key recovery attack than assumed by the submission.

The submitters responded by proposing a countermeasure that made the structure essentially the same as that of BIKE. NIST judged this to be too large a modification to consider the scheme for the third round.

In light of these reasons, NIST did not select LEDAcrypt to continue on.

3.12 NewHope

NewHope is a KEM based on the presumed hardness of the RLWE problem. At its core is Regev's original idea for public-key encryption from plain LWE but specialized to a power-of-2 cyclotomic ring structure, enabling smaller ciphertext and key sizes as well as fast computations via NTT. CCA security is achieved by a standard flavor of Fujisaki-Okamoto transform and is supported by proofs in the classical and quantum random oracle models. Among all LWE-based lattice submissions, NewHope (and other RLWE schemes) can be viewed as the most structured, with MLWE being an intermediately structured case and plain LWE being the least structured case. As a result of this structure, the scheme has very strong performance for nearly all applications.

In a technical sense, the security of NewHope is never better than that of KYBER. A recent paper gives a highly parameterizable, essentially linear-time reduction from RLWE to MLWE [23]. If that reduction is specialized to the case of NewHope, one finds the following: the reduction takes RLWE instances and outputs an MLWE instance; it is modulus-preserving; it is "almost" sample-preserving; it is error distribution-preserving; and it translates the ring dimension for RLWE into the product of ring-dimension times module-rank for MLWE. As such, any attack against an underlying MLWE instance implies a substantially similar-cost attack against NewHope's underlying RLWE instance. There are a few minor caveats. However, NIST does not expect that these issues will substantially change the relative concrete security situation of NewHope and an MLWE scheme (like KYBER) that is indicated by the presence of such a tight and efficient reduction.

Further, NIST observed that the CoreSVP strength estimates of NewHope and KYBER are substantially comparable, and KYBER was slightly more efficient in most benchmarks. Specifically because of the relaxation in algebraic structure, KYBER naturally supports a category 3 security strength parameter set, whereas NewHope does not.

Despite the numerous strengths of the NewHope KEM proposal, NIST developed a slight but clear preference for KYBER and for low-rank MLWE schemes over RLWE schemes for the KEM application setting. Therefore, NIST did not select NewHope to continue into the third round.

3.13 NTS-KEM

The NTS-KEM submission merged with Classic McEliece in February 2020. The two specifications were very similar. The merged team elected to adopt the Classic McEliece specification, as well as the name, for their merged submission. NIST appreciates the willingness of the two submission teams to work together.

3.14 ROLLO

At the start of Round 2, ROLLO was comprised of three rank metric code-based KEMs with security based on the rank syndrome decoding (RSD) problem. The first-round report noted that the strength of algebraic attacks against RSD was not well understood and should be explored.

Since then, new algebraic attacks have surfaced (see [40, 41]) that model the decoding problem as a system of multivariate equations using equations from the extension field structure to solve. The most recent algebraic attack is more efficient than combinatorial approaches against the parameter sets given in ROLLO, resulting in a near-complete break of all three KEMS. All security levels of ROLLO II and III were reduced to less than 128 bits of security, while the category 5 parameters of ROLLO I were reduced to category 1 security.

New parameter sets were proposed, resulting in a new ROLLO I scheme which achieves CPA security and a ROLLO II scheme which achieves CCA security, both with category 1, 3, and 5 security levels. The new ROLLO I public keys and ciphertexts are roughly 50 % larger than before, though they are both still significantly smaller than RQC. Although the new key and ciphertext sizes remain competitive, the security analysis of ROLLO needs more time to mature.

NIST did not select ROLLO to advance on in the PQC standardization process. Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth.

3.15 Round5

Round5 is a lattice-based scheme which offers parameter sets optimized for various use cases. The security is based on the (Ring) Learning With Rounding problems. An error-correcting code XE*f* is used to correct decryption failures, similar to the technique used by LAC, and CCA security is achieved by applying a Fujisaki-Okamoto transform. The performance of Round5 is impressive, both in bandwidth requirements and processing time. The unified design of Round5 allows it to be instantiated in either a ring or non-ring setting.

The security of Round5 was analyzed more closely during the second round, which led to two minor attacks [42, 43]. As a result, the team made small updates to the proposed parameter sets to protect against these attacks. During the second round, Round5 specified the use of TupleHash and TupleHashXOF to ensure domain separation. Small modifications were also made to further optimize implementations of Round5 and protect against side-channel attacks.

Overall, the Round5 specification is significantly more complicated than all of the other second-round candidates. Moreover, the Round5 submission documents did not offer a royalty-free license, and there are competing lattice-based schemes which do. The matrix A in Round5 is deterministically generated from a short seed using three different techniques, parametrized by τ in $\{0, 1, 2\}$. NIST only finds confidence in the security of one of the techniques ($\tau = 0$) and notes that there is no proof of security for the other two techniques.

For the reasons listed above, NIST does not view Round5 as more promising than the three lattice-based finalists selected. NIST seeks to focus the attention of the community on a small number of algorithms and so needed to cut the number of structured lattice schemes. Thus, even though Round5 has excellent performance, it was not selected to advance.

3.16 RQC

RQC is a structured rank metric code-based KEM with security based on the RSD problem targeting IND-CCA security. RQC differs from ROLLO in that it uses an LWE-like construction with a public error-correcting code instead of an NTRU style construction. This allows RQC to have a zero decryption failure rate, but it also requires larger ciphertexts than either variant of ROLLO. The first-round report noted that the strength of algebraic attacks against RSD was not well understood and should be explored. Since then, new algebraic attacks have surfaced which model the decoding problem as a system of multivariate equations using equations from the extension field structure to solve [40, 41]. The most recent algebraic attack is more efficient than combinatorial approaches against the parameter sets given in the round 2 specification of RQC, resulting in a near-complete break. All security levels of RQC were reduced to less than 128 bits of security.

New parameter sets were proposed to provide adequate security against algebraic attacks. These resulted in key and ciphertext sizes that were a little more than double what they were at the beginning of the second round. Although the new key and ciphertext sizes remain competitive (albeit less so than those of ROLLO), the security analysis of RQC needs more time to mature.

NIST did not select RQC to advance on in the PQC standardization process. Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth.

3.17 Three Bears

Three Bears is a KEM whose security is based on the presumed hardness of the Integer Module Learning With Errors (I-MLWE) problem, a new variant of the MLWE problem. It draws its inspiration from [30] and, more explicitly, from KYBER and related improvements to the MLWE-like design paradigm that have been devised over time. Three Bears is one of two examples of candidates that are a non-cyclotomic structured lattice KEM. The chosen polynomial ring underlying the module structure in Three Bears is isomorphic to the integers modulo a generalized Mersenne prime, and elements of the ring are written simply as (large) integers in the provided implementations. The scheme also uses an internal Melas forward error correcting code in all parameter sets. Altogether, this leads to a highly efficient scheme.

In the second round, the security proof sketch in the submission documentation was updated to a formal proof. In addition, parameters were slightly modified to lower the decryption failure rate, along with a detailed analysis for bounding the rate. A later tweak during the second round made implicit rejection mandatory in the specification.

NIST notes there is a security reduction which shows the asymptotic security equivalence of the usual notion of RLWE and Integer-RLWE, and this proof appears to carry directly over to the case of MLWE and I-MLWE. However, NIST notes that the I-MLWE hardness assumption was essentially created for the sake of submission to the NIST PQC standards process and has not undergone enough rigorous review by the broader cryptographic research community. While the reduction exists between I-MLWE and MLWE, there is still the possibility of concrete attacks exploiting the I-MLWE structure that are not fully captured by the security reduction, or other

new issues that may have not been discovered yet. In a similar vein, it seems that the entire Three Bears submission package appears to have received less attention by third-party researchers than other KEM submissions, particularly other lattice KEM submissions.

While NIST believes the technical and scientific merits of Three Bears are significant, this is not a substitute for a sufficient threshold of broader community attention. NIST therefore chose not to keep Three Bears under consideration for standardization, as there are other options which have comparable security and performance.

3.18 CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM was one of three lattice-based signature schemes in the second round. The security of DILITHIUM relies on the hardness of the MLWE and module short integer solutions problems (MSIS) and follows the *Fiat-Shamir with aborts* technique [44]. DILITHIUM uses the same modulus and ring for all parameter sets and samples via the uniform distribution, which results in a simpler implementation than its main competitor, FALCON.

Overall, DILITHIUM has strong, balanced performance in terms of key and signature sizes and in the efficiency of the key generation, signing, and verification algorithms. DILITHIUM performs well in real-world experiments.

For the second round, DILITHIUM added the option to generate a signature non-deterministically and added an implementation based on using AES rather than SHAKE to illustrate the future benefits of hardware instructions. In addition, new research on security in the QROM was published [45], which applies to DILITHIUM.

NIST encourages the DILITHIUM team to add a category 5 parameter set. More study is also needed on understanding the concrete security, as DILITHIUM has the lowest CoreSVP security strength parameter set of any of the lattice schemes still in the process. NIST selected DILITHIUM as a finalist and expects that either DILITHIUM or FALCON will be standardized as the primary post-quantum signature scheme at the conclusion of the third round.

3.19 FALCON

FALCON is a lattice-based signature scheme utilizing the “hash and sign” paradigm. Security is based on the hardness of the SIS (short integer solution) problem over NTRU lattices, and security proofs are given in both the random oracle model (ROM) and QROM with tight reductions. FALCON is more complex to implement than DILITHIUM, requiring tree data structures, extensive floating-point operations, and random sampling from several discrete Gaussian distributions.

One of the advantages of FALCON is that it offers the smallest bandwidth (public key size and signature size) of all of the second-round digital signature schemes. FALCON is also efficient in signing and verifying, although key generation is slower. FALCON can easily be put into existing protocols and applications and offers very good overall performance.

At the beginning of the second round, FALCON removed their category 3 parameter sets, which simplified their specification and implementation because they used a different modulus and ring

choice. The other major update during the second round was a constant-time implementation released shortly after NIST's 2nd PQC Standardization Conference.

During the third round, NIST encourages more scrutiny of FALCON's implementation to determine whether the use of floating-point arithmetic makes implementation errors more likely than other schemes or provides an avenue for side-channel attacks. In addition, it would be helpful to have test vectors for the sampler, perhaps by making it deterministic for a random seed, so that implementations can be verified using known answer tests (KATs). As with several other candidates, FALCON's category 1 parameters have relatively low CoreSVP security strength, and so further study is needed.

FALCON was selected as a third-round finalist. As stated above, NIST expects that either DILITHIUM or FALCON will be standardized as the primary post-quantum signature scheme at the conclusion of the third round.

3.20 Rainbow

Rainbow is a multivariate signature scheme with a layered construction based on the Unbalanced Oil-Vinegar (UOV) signature scheme. The additional structure imposed by the Rainbow layers exposes the scheme to a larger array of cryptanalytic techniques but improves the scheme's efficiency. Rainbow offers fast signing and verifying and very short signatures but has very large public keys.

The selection of Rainbow increases the diversity of the finalist signature schemes; however, due to the very large key size, Rainbow is not suitable as a general-purpose signature algorithm to replace algorithms that currently appear in FIPS 186-4. In particular, the large public keys make certificate chains extremely large. There are applications, however, which do not need to send keys very often. For such applications, Rainbow offers small and fast signatures. The only other advancing candidate signature with a similar performance profile, GeMSS, has substantially larger keys and appears to be difficult to implement on very low-end devices. For these reasons, Rainbow was selected as a finalist.

NIST researchers noted a gap between performance and theoretical complexity for a few attack avenues relevant to the Rainbow scheme. During the second round, some tighter theoretical analyses of (as well as new algorithms for) these well-known attacks have been published [41, 46]. In particular, [46] shows that a parameter tweak is necessary for all parameter sets to achieve the claimed levels of security. Still, with a more conservative parameter selection, it should be possible to meet the claimed security levels with minimal performance cost.

Before Rainbow can be ready for standardization, its parameters must be adjusted to ensure that it meets its claimed security targets. In addition, NIST prefers algorithms with royalty-free licensing in order to encourage widespread adoption.

3.21 GeMSS

GeMSS is a multivariate signature scheme constructed using the "big field" paradigm. GeMSS is based on the HFEv- construction originating in the late 1990s. The scheme utilizes a Fiestel-

Patarin construction to bootstrap EUF-CMA security from the assumed universal unforgeability of the HFEv- primitive.

GeMSS offers the smallest signatures of any digital signature candidate, supports a reasonably fast verification algorithm, and rests on a stable and well-studied mathematical problem. The drawbacks of the scheme include extremely large public keys, difficulty implementing the algorithm on low-end devices, and signing times ranging from slow to very slow. With these performance security characteristics, GeMSS seems to be a good and appropriate tool for applications in which offline signing and no transmission of the public key are acceptable and expected. GeMSS's large public keys may not work in many implementations of TLS and SSH without some implementation updates.

The second-round inclusion of the RedGeMSS and BlueGeMSS parameter sets offers additional flexibility in the performance properties over the initial submission package and appropriately addresses the concerns raised in [9]. It is possible that there may yet be additional trade-offs to further improve performance. In particular, the consideration of the number of bit operations involved in a hash collision attack may warrant a reevaluation of the number of iterations required in the Fiestel-Patarin transformation. As with Rainbow, ROLLO, and RQC, the complexity of some key recovery attacks against GeMSS was affected by recent progress on algebraic methods for solving MinRank [41]. However, this research did not contradict the claimed security of any of GeMSS's proposed parameter sets.

GeMSS competes most closely with Rainbow, another multivariate signature scheme with large keys and small signatures. GeMSS has much bigger public keys and much slower signing in exchange for slightly smaller signatures; Rainbow's performance profile is more appealing for most applications, and GeMSS appears to be difficult to implement on low-end devices. GeMSS is also based on a different security assumption. NIST sees GeMSS as an option for standardization if developments during the third round show Rainbow to be unacceptable for standardization. For these reasons, GeMSS was chosen as an alternative candidate.

3.22 Picnic

Picnic is a signature scheme that uses no number-theoretic or structured hardness assumptions. The security of Picnic depends on a random oracle assumption on the underlying hash function and on the security of the LowMC block cipher [47] against an adversary given a single plaintext/ciphertext pair. A Picnic signature is a non-interactive zero-knowledge proof of knowledge of the secret key. The message being signed is incorporated (via hashing) into the challenges of the proof of knowledge in such a way that only the holder of the secret key can produce the proof. The length of the signature depends on the multiplicative complexity of the encryption scheme and the specific technique to construct a zero-knowledge proof of knowledge (from the field of secure multi-party computation [48]). Picnic has small public key size, large signatures, and slow signing and verifying. Additionally, it appears that a straightforward implementation would have significant side-channel issues [49]. The second-round submission included analyses in the QROM model for each variant of PICNIC.

Picnic is a highly modular design. The cryptographic primitives—a hash function and block cipher—could be instantiated in different ways. The submitted design uses LowMC, a block

cipher designed to have low multiplicative complexity. LowMC has not been studied as much as AES and hence needs much more analysis before it can be standardized by NIST. However, the security requirements for the underlying block cipher in Picnic are much less stringent than the general security requirements of a block cipher—only a single plaintext/ciphertext pair is ever revealed, and an attacker needs to find a key that maps that plaintext to that ciphertext in order to forge Picnic signatures. Variants of Picnic based on AES have been proposed [50], but these lead to much larger signatures.

The approach to designing a signature scheme used in Picnic is quite new, and the design is evolving rapidly. Changes to the parameters and underlying proof of knowledge made during the second round improved performance significantly while fixing attacks discovered in the first round. NIST sees Picnic as an algorithm that is not yet mature enough to be standardized but which has the potential to improve a great deal in both performance and confidence in its security in the near future. NIST also sees Picnic's reliance on only assumptions about symmetric primitives as an advantage in case the need arises for an extremely conservative signature standard in the future. For this reason, Picnic was not selected as a finalist but was included as an alternate candidate.

3.23 SPHINCS+

SPHINCS+ is a stateless hash-based signature scheme. Its security is based entirely on assumptions about the security of the underlying hash function. There is a proof of security for all variants of SPHINCS+ in the random oracle model. There is also a standard-model proof for the robust variants based on plausible but nonstandard assumptions regarding a tweakable hash function constructed from the underlying hash. This proof assumes that the tweakable hash functions have post-quantum single function, multi-target collision resistance for distinct tweaks and post-quantum single function, multi-target decisional second-preimage resistance for distinct tweaks. Hash-based signatures are a very old technology dating back to the dawn of public key cryptography, so they have seen many decades of analysis. In general, SPHINCS+ is probably the least likely of any post-quantum signature candidate to be broken cryptanalytically. On the other hand, the design of SPHINCS+ makes it especially vulnerable to fault attacks [51, 52] and, to a lesser extent, side-channel attacks.

SPHINCS+ is a mature design with a thorough and clear specification. SPHINCS+ provides very solid assurance of its security claims, but this comes at a substantial cost in performance—it is slower, and its signatures are considerably larger than most other signature schemes. For example, for category 1 security, the shortest available SPHINCS+ signatures are four times the size of Dilithium signatures and require more than a thousand times the computation to produce. By contrast, SPHINCS+ public keys are very small—down to 32 bytes for category 1 security.

SPHINCS+ is defined with many different parameter sets offering different trade-offs between speed and signature size at security categories 1, 3, and 5. SPHINCS+ also added "simple" variants in round two, which provide improved speed for signing and verifying at the cost of security being proven only in the random oracle model. Some parameter sets require the use of a non-standard algorithm (Haraka [53]); if SPHINCS+ is eventually chosen as a standard, NIST does not foresee standardizing those parameter sets. The performance profile of SPHINCS+ means that dropping it into existing systems which now use RSA or ECDSA signatures would

not work well; extensive re-engineering would likely be necessary. It is difficult to imagine TLS with SPHINCS+ as the signature algorithm providing acceptable performance. Both the speed and size of signatures would be unacceptable.

NIST sees SPHINCS+ as an extremely conservative choice for standardization. If NIST's confidence in better performing signature algorithms is shaken by new analysis , SPHINCS+ could provide an immediately available algorithm for standardization at the end of the third round. Further, if NIST sees the need for an additional signature algorithm for applications that need very high security and can tolerate larger and slower signatures, NIST may decide to standardize SPHINCS+ in the future.

3.24 LUOV

LUOV is a multivariate signature scheme of the "small field" variety. LUOV is based on the UOV signature scheme that has remained secure and unchanged for over twenty years. The L in the name stands for "Lifted" and specifies the main innovation of the design. The keys of LUOV are far smaller than UOV keys with the same parameters because the coefficients of the keys of LUOV are depressed into a subfield.

During the second round, it was shown that the lifting modification is generically weak for sufficiently underdefined systems due to a new type of differential attack (see [54]). The second-round parameter sets of LUOV were significantly affected by this approach, undermining confidence in this methodology for any sufficiently underdefined polynomial system.

NIST did not select LUOV to advance to the third round. The development of the aforementioned attacks shows that the lifting innovation is too new to be incorporated into a standard at this time; however, there is room for growth in this area. The attack of [54] relies on the lifting degree as well as the imbalance in the number of polynomials and unknowns in the key. LUOV has already inspired the application of field lifting for other schemes [55], and while it is premature to either trust or discard the lifting construction, NIST believes there is value in the development of the science in this direction.

3.25 MQDSS

MQDSS is a multivariate digital signature scheme constructed via a Fiat-Shamir transform on a provably secure 5-pass identification scheme based on the multivariate quadratic (MQ) problem. Due to its construction, MQDSS is more directly comparable in structure and performance to symmetric-based signature schemes than other multivariate candidates.

During the second round, MQDSS suffered a forgery attack [56] that undermined the security claims for the submitted parameters. While the attack did not invalidate the proof of security for MQDSS, the practical effect of the attack is that 40 % more rounds and 50 % larger keys are required.

Even before the attack, MQDSS seemed to offer performance comparable but inferior to the most similar round 2 candidates, Picnic and SPHINCS+. The performance impact of the attack, however, renders MQDSS uncompetitive with Picnic and SPHINCS+. For this reason, MQDSS was not selected for inclusion among the round 3 candidates.

3.26 qTESLA

qTESLA is a digital signature scheme based on structured lattice assumptions. The public keys in qTESLA consist of LWE samples within a ring**,** and signing is done using hash functions and the "Fiat-Shamir with aborts" technique referred to above. The second-round version of qTESLA that was submitted to NIST specified 12 different parameter sets (q-TESLA-*, q-TESLA-*-s, and q-TESLA-p-*). After questions were raised about the security arguments in the specification [57], the authors retracted 10 of the parameter sets and kept the remaining two (q-TESLA-p-I and q-TESLA-p-III).

Although there is a benefit to having a diversity of design among lattice-based candidates, the performance of the remaining parameter sets of qTESLA is not strong enough to remain competitive. In particular, the public key sizes of q-TESLA-p-I and q-TESLA-p-III are about 15 to 20 times as large as those of FALCON and CRYSTALS-DILITHIUM, and the signature sizes are larger as well. In comparing cycle counts required for signing and verifying, qTESLA is roughly 2 to 5 times slower than FALCON and CRYSTALS-DILITHIUM. For these reasons, qTESLA is not advancing to the third round.

4 Conclusion

The internal and external cryptanalysis, performance benchmarks, studies, and experiments involving the second-round candidates led NIST to the selection of seven third-round finalists and eight alternate candidates. The announcement of these schemes marks the beginning of the third round of the NIST PQC Standardization Process. This decision was difficult as several eliminated schemes are based on novel ideas or research areas which are still worthy of continued study.

As CRYSTALS-KYBER, NTRU, and SABER are all structured lattice schemes, NIST intends to select, at most, one of these finalists to be standardized. The same is true for the finalist signature schemes CRYSTALS-DILITHIUM and FALCON. In NIST's current view, these structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes. Nonetheless, NIST believes it is prudent to continue to study schemes that are not based on structured lattices as a hedge against unexpected progress in cryptanalysis. This is particularly true for digital signature schemes where the best schemes that are not based on structured lattices have a substantial performance penalty for general-purpose use.

For the eight alternate candidate algorithms advancing to the third round, NIST notes that these algorithms still may potentially be standardized; although that most likely will not occur at the end of the third round. NIST expects to have a fourth round of evaluation for some of the candidates on this track.

If new results emerge during the third round which undermine NIST's confidence in some of the finalists, NIST may extend the timeline, or make changes to the process. If NIST has less serious concerns specific to a particular finalist and sees the need to continue evaluating it, NIST may instead defer the decision about standardization for the affected finalist until the fourth round.

The third round is expected to last 12-18 months. Submission modifications should be submitted to NIST by October 1, 2020, in a complete submission package as defined in [33]. It would be helpful if submission teams provided NIST with a summary of their expected changes by August 10, 2020. As a general guideline, NIST expects that any modifications to the seven finalists should be relatively minor while allowing more latitude to the eight additional candidate algorithms. Note, however, that larger changes may signal that an algorithm is not mature enough for standardization at this time. More detailed instructions will be provided.

The efforts of the cryptographic community have been invaluable in analyzing and implementing schemes throughout this process. NIST hopes that with only seven finalists and eight alternate candidates, the public review period will include more work on side-channel resistant implementations, performance data in internet protocols, and performance data for hardware implementations in addition to more rigorous cryptanalytical study. NIST is grateful to the community for all of the research, support, and analysis provided.

NIST plans to host a Third NIST PQC Standardization Conference in the spring or summer of 2021. More details will be provided at a later date. NIST expects to select a small number of

candidates for standardization by early 2022. To achieve this goal, the third round will serve as a final round for the first phase of standardization, though some schemes will remain under consideration for future standards.

NIST is pleased with the progress of the PQC standardization effort but recognizes that current and future research may lead to promising schemes which were not part of the NIST PQC Standardization Project. NIST may adopt a mechanism to accept such proposals at a later date. In particular, NIST would be interested in a general-purpose digital signature scheme which is not based on structured lattices.

References

[1] National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

[2] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[3] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2

[4] "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms", 81 *Federal Register* 92787 (December 20, 2016), pp. 92787-92788. https://federalregister.gov/d/2016-30615

[5] Moody D (2016) Post-Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions. *International Conference on Post-Quantum Cryptography - PQCrypto.* Available at https://csrc.nist.gov/Presentations/2016/Announcement-and-outline-of-NIST-s-Call-for-Submis

[6] Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner RA, Smith-Tone D (2016) Report on Post-Quantum Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105. https://doi.org/10.6028/NIST.IR.8105

[7] "Request for Comments on Post-Quantum Cryptography Requirements and Evaluation Criteria", 81 *Federal Register* 50686 (August 2, 2016), pp. 50686-50687. https://federalregister.gov/d/2016-18150

[8] Workshop on Cybersecurity in a Post-Quantum World. National Institute of Standards and Technology, Gaithersburg, Maryland, April 2-3, 2015. Available at https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-a-Post-Quantum-World.

[9] Alagic G, Alperin-Sheriff J, Apon D, Cooper DA, Dang QH, Miller CA, Moody D, Peralta R, Perlner RA, Robinson A, Smith-Tone D, Liu Y-K (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240. https://doi.org/10.6028/NIST.IR.8240

[10] National Institute of Standards and Technology (2016) *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[11] Guo Q, Johansson T, Nilsson A (2020) A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/743

[12] Bernstein D, Lange T (eds.), *eBACS: ECRYPT Benchmarking of Cryptographic Systems - SUPERCOP* (2020). Available at https://bench.cr.yp.to/supercop.html

[13] Florida Atlantic University (2020), *PQC-Wiki*. Available at https://pqc-wiki.fau.edu/w/Special:DatabaseHome

[14] PQShield (2020), *PQCzoo*. Available at https://pqczoo.com

[15] *PQClean* (2020). Available at https://github.com/PQClean/PQClean

[16] *pqm4: Post-quantum crypto library for the ARM Cortex-M4* (2020). Available at https://github.com/mupq/pqm4

[17] McEliece R (1978) A public-key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report*, DSN PR 42-44. NASA. Available at https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[18] Hülsing A, Ning K-C, Schwabe P, Weber F, Zimmermann PR (2020) Post-quantum WireGuard. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/379

[19] Regev O (2004) New lattice-based cryptographic constructions, Journal of the ACM, 51(6): 899-942. https://doi.org/10.1145/1039488.1039490.

[20] Eiichiro F, Okamoto T (1999) Secure Integration of Asymmetric and Symmetric Encryption Schemes. *Annual International Cryptology Conference - CRYPTO* (Springer), pp. 537-544. https://doi.org/10.5555/646764.706343

[21] Hofheinz D, Hövelmanns K, Kiltz E (2017) A Modular Analysis of the Fujisaki-Okamoto Transformation. *Theory of Cryptography Conference* (Springer), pp. 341-371. https://doi.org/10.1007/978-3-319-70500-2_12

[22] Ravi P, Roy D, Bhasin S, Chattopadhyay A, Mukhopadhyay D (2019) Number "Not Used" Once - Practical Fault Attack on pqm4 Implementations of NIST Candidates. *International Workshop on Constructive Side-Channel Analysis and Secure Design* (Springer), pp. 232-250. https://doi.org/10.1007/978-3-030-16350-1_13

[23] Peikert C, Pepin Z (2019) Algebraically Structured LWE Revisited. *Theory of Cryptography Conference* (Springer), pp. 1-23. https://doi.org/10.1007/978-3-030-36030-6_1

[24] Erdem A, Ducas L, Pöppelmann T, Schwabe P (2016) Post-quantum key exchange—a new hope. *USENIX Security Symposium* (USENIX association), pp. 327-343. https://doi.org/10.5555/3241094.3241120

[25] Institute of Electrical and Electronics Engineers (2009) *IEEE Standard 1363.1-2008 - Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices* (IEEE, Piscataway, New Jersey, United States). https://doi.org/10.1109/IEEESTD.2009.4800404

[26] American National Standards Institute (2010) *ANSI X9.98-2010 -Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry* (ANSI, New York City, United States). Available at https://webstore.ansi.org/standards/ascx9/ansix9982010r2017

[27] Sendrier N, Vasseur V. (2020) About low DFR for QC-MDPC decoding. *International Conference on Post-Quantum Cryptography – PQCrypto* (Springer), pp. 20-34. https://doi.org/10.1007/978-3-030-44223-1_2

[28] Drucker N, Gueron S, Kostic D (2020) QC-MDPC decoders with several shades of gray. *International Conference on Post-Quantum Cryptography - PQCrypto* (Springer), pp. 35-50. https://doi.org/10.1007/978-3-030-44223-1_3

[29] Dachman-Soled D, Ducas L, Gong H, Rossi M (2020) LWE with Side Information: Attacks and Concrete Security Estimation. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/292

[30] Lyubashevsky V, Peikert C, Regev O (2010) On Ideal Lattices and Learning with Errors over Rings. *Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT* (Springer), pp. 1-23. https://doi.org/10.1007/978-3-642-12190-5_1

[31] Peikert C, Regev O, Stephens-Davidowitz N (2017) Pseudorandomness of Ring-LWE for Any Ring and Modulus. *Annual ACM Symposium on the Theory of Computing Proceedings - STOC* (ACM), pp. 461-473. https://doi.org/10.1145/3055399.3055489

[32] Jaques S, Schanck J (2019) Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE. *Annual International Cryptology Conference - CRYPTO* (Springer), pp. 32-61. https://doi.org/10.1007/978-3-030-26948-7_2

[33] Adj G, Cervantes-Vázquez D, Chi-Domínguez JJ, Menezes A, Rodríguez-Henríquez F (2019) On the Cost of Computing Isogenies Between Supersingular Elliptic Curves. *International Conference on Selected Areas in Cryptography - SAC* (Springer), pp. 322-343. https://doi.org/10.1007/978-3-030-10970-7_15

[34] Aurélien G, Montoya S, Renault G (2020) Attack on LAC Key Exchange in Misuse Situation. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/063

[35] D'Anvers JP, Tiepelt M, Vercauteren F, Verbauwhede I, (2019) Timing attacks on error correcting codes in post-quantum secure schemes. *ACM Workshop on Theory of Implementation Security Workshop – TIS* (ACM), pp. 2-9. https://doi.org/10.1145/3338467.3358948

[36] Greuet A, Montoya S, Renault G (2020) Attack on LAC Key Exchange in Misuse Situation. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/063

[37] Guo Q, Johansson T, Yang J (2019) A Novel CCA Attack using Decryption Errors against LAC. *Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT* (Springer), pp. 82-111. https://doi.org/10.1007/978-3-030-34578-5_4

[38] Post-Quantum Cryptography Submissions, Public Comments on LAC. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/LAC-official-comment.pdf, https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-2/official-comments/LAC-round2-official-comment.pdf

[39] Apon D, Perlner R, Robinson A (2020) Cryptanalysis of LEDAcrypt. *Cryptology ePrint archive preprint*. https://eprint.iacr.org/2020/455

[40] Bardet M, Briaud P, Bros M, Gaborit P, Neiger V, Ruatta O, Tillich JP (2020) An Algebraic Attack on Rank Metric Code-Based Cryptosystems. *Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT* (Springer), pp. 64-93. https://doi.org/10.1007/978-3-030-45727-3_3

[41] Bardet M, Bros M, Cabarcas D, Gaborit P, Perlner R, Smith-Tone D, Tillich JP, Verbel J (2002) Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems. *arXiv preprint*. https://arxiv.org/abs/2002.08322

[42] Son Y (2019) A Note on Parameter Choices of Round5. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2019/949

[43] Son Y, Cheon JH (2019) Revisiting the Hybrid attack on sparse and ternary secret LWE. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2019/1019

[44] Lyubashevsly V (2009) Fiat-Shamir with aborts: Applications to Lattice and Factoring-Based Signatures. *International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT* (Springer), pp. 598-616. https://doi.org/10.1007/978-3-642-10366-7_35

[45] Don J, Fehr S, Majenz C, Schaffner C (2019) Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model. *Annual International Cryptology Conference - CRYPTO* (Springer), pp. 356-383. https://doi.org/10.1007/978-3-030-26951-7_13

[46] Smith-Tone D, Perlner R (2020) *Rainbow Band Separation is Better than we Thought*. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/702

[47] Albrecht M, Rechberger C, Schneider T, Tiessen T, Zohner M (2015) Ciphers for MPC and FHE. *Annual International Conference on the Theory and Applications of Cryptographic Techniques- EUROCRYPT* (Springer), pp. 430-454. https://doi.org/10.1007/978-3-662-46800-5_17

[48] Ishai Y, Kushilevitz E, Ostrovsky R, Sahai A (2007) Zero-Knowledge from Secure Multiparty Computation. *ACM Symposium on Theory of Computing - STOC* (ACM), pp. 21-30. https://doi.org/10.1145/1250790.1250794

[49] Gellersen T, Seker O, Eisenbarth T (2020) Differential Power Analysis of the Picnic Signature Scheme. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2020/267

[50] Guilhem C, Meyer L, Orsini E, Smart N (2019) BBQ: Using AES in Picnic Signatures. *International Conference on Selected Areas in Cryptography – SAC* (Springer), pp. 669-692. https://doi.org/10.1007/978-3-030-38471-5_27

[51] Laurent C, Martinelliand A, Prest T (2018) Grafting Trees: A Fault Attack against the SPHINCS framework. *International Conference on Post-Quantum Cryptography -PQCrypto* (Springer), pp. 165-184. https://doi.org/10.1007/978-3-319-79063-3_8

[52] Genêt A, Kannwischer MJ, Pelletier H, McLauchlan A (2018) Practical Fault Injection Attacks on SPHINCS. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2018/674

[53] Kölbl S, Lauridsen M M, Mendel F, Rechberger C (2016) Haraka v2 – Efficient Short-Input Hashing for Post-Quantum Applications. *IACR Transactions on Symmetric Cryptology*, 2016(2):1-29. https://doi.org/10.13154/tosc.v2016.i2.1-29

[54] Ding J, Deaton J, Schmidt K, Vishakha, Zhang Z (2019) Cryptanalysis of The Lifted Unbalanced Oil Vinegar Signature Scheme. *Cryptology ePrint Archive preprint*. https://eprint.iacr.org/2019/1490

[55] Duong D H, Van Luyen L, Tran HTN (2020) Choosing subfields for LUOV and lifting fields for rainbow. *IET Information Security*, 14(2):196-201. https://doi.org/10.1049/iet-ifs.2018.5288

[56] Kales D, Zaverucha G (2020) Forgery Attacks on MQDSSv2.0. Post-Quantum Cryptography Round 2 Submissions, Public Comments on MQDSS. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-

Quantum-Cryptography/documents/round-2/official-comments/MQDSS-round2-official-comment.pdf

[57] Post-Quantum Cryptography Round 2 Submissions, Public Comments on qTESLA. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/official-comments/qTESLA-round2-official-comment.pdf