Manuscript submitted to
AIMS' Journals
Volume **X**, Number **0X**, XX **200X**

doi:10.3934/xx.xx.xx.xx

pp. **X–XX**

NEW MISSION AND OPPORTUNITY FOR MATHEMATICS RESEARCHERS: CRYPTOGRAPHY IN THE QUANTUM ERA

Lily Chen* and Dustin Moody

Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD 20899, USA

(Communicated by the associate editor name)

Abstract. This article introduces the NIST post-quantum cryptography standardization process. We highlight the challenges, discuss the mathematical problems in the proposed post-quantum cryptographic algorithms and the opportunities for mathematics researchers to contribute.

1. **Public-Key Cryptography and Quantum Challenges.** Since its invention in 1976, public-key cryptography has greatly rejuvenated many areas of mathematics, such as number theory and finite fields for their applications in cryptography. Today, the most widely deployed public key cryptography schemes (RSA encryption, RSA signatures, Diffie-Hellman key agreement, Elliptic Curve Digital Signature Algorithms) are either based on the hardness of integer factorization or the discrete logarithm problem. By hardness we mean no polynomial time algorithms have been found to solve the problems. Since the 1990s, the National Institute of Standards and Technology (NIST) has published public-key cryptography standards through Federal Information Processing Standards (FIPS) 186 [16] for signatures and NIST Special Publications (SP) 800-56A and 800-56B [11, 12] for key establishment. These standards have been widely implemented in communication networks and digital devices, which have served as the cornerstone of cybersecurity.

The hardness of the integer factorization and discrete logarithm problems is believed to provide sufficient security, as long as they can only be attacked using classical computing technology. However, Peter Shor's astounding results [13] show that with quantum computers, factorization and discrete logarithms can be solved in polynomial time. That is, the arrival of quantum computers will fatally shake the security of all widely deployed public-key cryptographic schemes.

Besides public-key cryptography, NIST cryptographic standards also cover symmetric-key based cryptographic algorithms such as block ciphers [17] and message authentication codes [18]. For symmetric-key based cryptosystems, there is also an impact on security as a result of quantum computers. Using Grover's algorithm [7], there is a square root speed up which reduces the key search complexity from 2^n to $2^{n/2}$ for a block cipher with an n-bit key. The quantum impact on symmetric-key based

2010 *Mathematics Subject Classification.* Primary: 11T71, 14G50; Secondary: 94A60.

Key words and phrases. Post-quantum cryptography, public-key cryptography, mathematical research, standarization, quantum-safe, quantum resistant.

* Corresponding author:

cryptography can be handled by simply increasing the key size, until a quantum complexity of $2^{n/2}$ is considered infeasible to launch an attack. In this article, we therefore focus our discussion on public-key cryptography.

In dealing with the quantum challenge, a first question is whether there are any problems which remain hard, even in the face of quantum computers. And if yes, then whether a cryptographic mechanism can be built whose security is based on both the classical and quantum hardness of the problem. We will discuss these problems in the next section.

2. **Post-Quantum Cryptography.**

In fact, even though the most widely deployed public-key cryptographic mechanisms are either based on the integer factorization or discrete logarithm problem, they are certainly not the only hard problems upon which public-key cryptosystems have been based. Even in the 1970s, other public-key cryptography mechanisms were proposed with different security assumptions. One example is the McEliece cryptosystem [9]. It is related to the hardness of decoding a general linear code, which is classically believed to be hard and seems immune to Shor's quantum attack. The original algorithm used binary Goppa codes, and it never gained much acceptance in the cryptographic community for its overly large size of public keys. At the time when public-key cryptography was first deployed, the computing capacity and communication bandwidth were far more limited in comparison with today's technology. In addition, there were other systems, like the knapsack cryptosystem [2], which were not adopted due to security flaws.

In 1996, the NTRU cryptosystem [8] was proposed by three mathematicians from Brown University based on certain hard problems involving lattices. NTRU included both an encryption and digital signature mechanism, a feature shared by the popular RSA cryptosystem in which encryption and signatures use the same operations. Even though the original NTRU signature mechanism was broken [6], its encryption algorithm is still believed to be secure (even against quantum attacks).

Ever since it was known that large-scale quantum computers would threaten our currently deployed public-key cryptosystems, researchers have looked for schemes which can resist both classical and quantum attacks. This field has come to be known as post-quantum cryptography, also known as quantum-resistant or quantum-safe cryptography.

Over the past decade, post-quantum cryptography has become arguably the most active area in cryptography. It has attracted researchers in mathematics, computer science, and quantum information among other areas. Hundreds of papers are presented, published, and released each year.

To design new cryptographic algorithms which are able to resist quantum computers, researchers first look for hard mathematical problems upon which cryptographic mechanisms can be built. Besides the previously mentioned hard problems involving lattices and coding, other problems and structures have been explored. For example, solving a non-linear system of multivariate polynomial equations or recovering an unknown isogeny between a pair of supersingular elliptic curves.

While historically many public-key cryptographic systems have relied on using an algebraic or number theoretical problem, so called hash-based signatures use the one-wayness of cryptographic hash functions [5]. This idea was proposed in the 1970s to build one-time signatures. The concept was later extended to more general signature schemes known as stateful hash-based signatures. The internal

state must be carefully managed to ensure that each private key can be used only once to generate a signature. More recently, stateless hash-based signatures have been proposed, which do not require managing the state at all.

Among the various categories being researched for post-quantum cryptography, some are relatively new while others are based on ideas known for many years. Research in these areas has involved establishing security based on several different assumptions, as well as optimizing for efficiency by including more algebraic structure in an effort to reduce parameter sizes.

Informally, when we say the security of a cryptographic mechanism $\mathcal{A}$ is based on a certain hard problem $\mathcal{B}$, we mean there is a reduction proof which shows that breaking the mechanism $\mathcal{A}$ implies finding an efficient algorithm to solve the problem $\mathcal{B}$. Here 'breaking' means an algorithm violates some pre-defined security definition, such as being secure against chosen ciphertext attacks for public-key encryption algorithms. To prove a mechanism quantum secure, it must be understood what is meant by the statement that a problem is 'quantum hard'. It usually just means that nobody has found a quantum algorithm to efficiently solve it (i.e. in polynomial time). We note that Shor's algorithm is not a generic black-box approach. That is, it exploits some of the structure inherent in the factorization and discrete logarithm problems, and cannot be trivially applied to other problems. Even though it is believed that there are no polynomial time quantum algorithms to solve NP-complete problems [1], most of the assumptions used in post-quantum cryptography are variations of hard problems which have not been proven to be NP-hard. The theory to support the security of post-quantum cryptography algorithms is far from being perfect, which leaves a large space for researchers to explore.

When a cryptographic algorithm is actually implemented in an application, the practical security is even more complicated. Over the past few decades, we have observed countless failures showing that security flaws can be exploited in many ways. For example, an improper padding method can leak information about the plaintext. As another example, it has been demonstrated that carefully observing resource consumption or timing information can lead to side-channel attacks. Most post-quantum cryptography mechanisms presented in the literature are relatively new, and numerous details must be investigated before they can be safely adopted for practical applications.

Besides security, a second factor to determine whether a cryptographic algorithm can be used in a given application environment is its efficiency. Performance is not only counted by an algorithm's processing speed but also the communication overhead and memory requirements: key sizes, data expansion rate (i.e. ciphertext size), signature size etc. For a post-quantum cryptography mechanism, many elements, such as incorporating algebraic structure and the selection of concrete parameters, can impact the performance. For example, schemes based on more structured assumptions tend to have smaller keys. However, those assumptions are frequently not proven to be equivalent to the corresponding generic assumptions. Designers are faced with the dilemma of taking a conservative approach in regards to security or a more aggressive approach which optimizes performance.

As we can see, there are a considerable number of topics in post-quantum cryptography which need to be explored by researchers and it will likely take many years to get some of the most important questions answered. However, with the significant progress being made in building quantum computers, it is more and more urgent to replace the currently deployed public-key cryptography tools with

quantum-resistant counterparts. It usually takes several years to develop standards, besides who can say how many years for industry to make a migration to new cryptographic mechanisms. In the next section, we will introduce NIST's initiative in regard to the standardization of post-quantum cryptography.

3. NIST's Standardization Approach.

NIST started to develop cryptographic standards in the 1970s, with the first cryptographic standard the Data Encryption Standard (DES) [14]. At that time, confidentiality was the most critical objective for information security. When the security of DES was not sufficient any more [4], NIST initiated a competition from 1997 to 2000 to select a new block cipher for standardization. The competition was open to researchers worldwide to submit their designs for block ciphers. The Advanced Encryption Standard (AES) was selected among 15 second round candidates and published in FIPS 197. Today, AES has been implemented in almost every piece of communication equipment and digital device.

Another essential cryptographic primitive is a hash function. Hash functions are used for digital signatures, message authentication codes, key derivation functions and many other cryptographic purposes. The SHA-1 and SHA-2 hash function families are specified in FIPS 180-4 [15]. In 2005, the first practical attack on SHA-1 was presented. To make sure the hash function standards could provide sufficient security, in 2007 NIST organized a competition through which NIST selected the SHA-3 family of hash functions. SHA-3 was standardized in FIPS 202 [19], to complement the SHA-2 family of hash functions.

Both the AES and SHA-3 competitions were very successful and cryptographic competitions became a well-accepted procedure to select major cryptographic primitives for standardization. A natural question is whether a competition would be a good approach in selecting post-quantum cryptography mechanisms for standardization.

To answer this question, we need to understand the scope of post-quantum cryptography standardization. NIST public-key cryptography standards cover only the most essential functions: public-key encryption, key agreement, and digital signature. Thus first and foremost, the scope for post-quantum cryptography standardization is to find quantum-resistant replacements for these three main functions. The three different functions are in contrast to previous competitions which were looking at only one functionality (block cipher or hash function). Second, post-quantum cryptography is a new and active area. The understanding of both the security and performance, as we discussed in the previous section, is far from being complete. Thus, narrowing down a candidate pool of algorithms may not precisely reflect a fair comparison among the candidates. Studying the literature, it is easily observed that each post-quantum mechanism seems to have both advantages and also inescapable disadvantages, which may make it hard to find a perfect winner for each cryptographic function. Also, to protect against potential attacks against schemes which may not have been thoroughly scrutinized enough, more than one candidate may be needed for each function to satisfy the requirements of different applications. The procedure is full of uncertainty and demands extraordinary collaboration among researchers. The competitive atmosphere may not be conducive to helping standardize the best designed mechanisms.

Nonetheless, NIST announced its plan of initiating post-quantum cryptography standards through a competition-like process at the PQCrypto 2016 conference

[10]. The announcement clearly indicated that the algorithms to be standardized would be solicited through a call for proposals worldwide. In the procedure of developing submission criteria, NIST released draft acceptability requirements and evaluation criteria for public comments before the final announcement [3]. Many of the comments NIST received very much reflected the major challenges which we will discuss throughout the rest of this section.

For post-quantum cryptography, the uncertainty of quantum security measurement is probably the most vexing problem. In today's cryptographic standards, classical security is specified by the complexity of the best-known algorithms in solving the underlying hard problem. For example, for the RSA cryptosystem, the security strength is measured by the complexity of the best factorization algorithm in regard to the binary length of the public key parameter n. In contrast, the security of post-quantum cryptographic mechanisms is based on various hard problems under the consideration of both classical and quantum computers. When using classical methods, one may or may not be able to use the quantum Grover's algorithm to speed up the computation. Furthermore, the quantum security requirements must be based on certain assumptions on future quantum computers including memory spaces and circuit depth. There does not seem to be a straightforward way to set requirements on security strength with a number of bits as NIST has done for classical security strengths.

As a result, NIST included five security categories in the final call for proposals. In each of the categories as shown in Table 1, classical and quantum security were related to the hardness of breaking a NIST standardized block cipher or hash function. The theory of security proofs in cryptography has advanced significantly in the past 20 years. During this time when we are looking for quantum-resistant cryptography mechanisms, security proofs with a standard definition have become part of the general approach for the assessment of a new cryptographic algorithms. The Call for Proposals states NIST's intent to standardize one or more schemes that enable 'semantically secure' encryption or key encapsulation with respect to adaptive chosen ciphertext attack (IND-CCA2) and existentially unforgeable digital signatures with respect to an adaptive chosen message attack (EUF-CMA). The notion of secure against chosen plaintext attack (IND-CPA) can be used for encryption or key establishment if it is to be employed in a purely ephemeral-key protocol. These security definitions are what NIST will consider to be a relevant attack. Submitters were encouraged to provide a security proof, although this was not required.

TABLE 1. Security Categories

Categories	**Security Description**
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Post-quantum cryptography mechanisms must also deal with many issues which haven't occurred in the current widely used public-key cryptography standards. For example, decryption failure happens in some post-quantum encryption mechanisms.

Even though it usually only happens with a very small probability, it needs to be checked that it does not introduce any security flaws when instantiated in any particular protocol. As another example, some encryption mechanisms have security vulnerabilities if a public key is re-used more than one time, and so cannot be used in applications which have static keys.

An increasingly important security feature is protection against side-channel attacks. Certain countermeasures can be applied to resist side-channel attacks, but may have a significant impact on the efficiency. The NIST call for proposals encourages the incorporation of countermeasures such as constant-time implementation optimized code, so that measured performance will more meaningfully reflect the performance of a secure implementation.

The procedure of developing the NIST requirements and criteria engaged the research community to work together. Many details, which had not been investigated before, emerged and needed to be considered and clarified. While the community pursued consensus, frequently there were several different opinions presented.

4. **Analysis and Evaluation.** By the deadline for submission at the end of November 2017, NIST received a total of 82 submissions with design team members from 25 countries on 6 continents. After checking for 'complete and proper' submissions against the published requirements, 69 were accepted as the first-round candidates, which were announced in December 2017. The candidates were publicly posted on the NIST website. Cryptographers immediately busied themselves in the security analysis of the submitted candidates. Within two months, 5 candidates were acknowledged as broken and withdrew from the process. Several other candidates had been attacked to various degrees. The 64 remaining first-round candidates were distributed into the major categories as indicated in Table 2.

TABLE 2. Distribution of First Round Candidates

	Signature	**Encryption/KEM**	**Overall**
Lattice-based	5	21	26
Code-based	2	17	19
Multivariate	7	2	9
Symmetric/Hash-based	3	0	3
Other	2	5	7
Total	19	45	64

NIST held the first NIST Post-Quantum Cryptography Standardization Conference in April 2018 [20]. There were 52 presentations covering 60 of the submitted algorithms. Each team presented design rationale with highlights on their advantages, shortcomings, and differences with the other submissions.

The analysis and evaluation of the first-round candidates greatly promoted research in the field, bringing about numerous results published in the literature. Researchers also submitted analysis and evaluation on candidates through publicly-shared official comments on the NIST website. More than three hundred comments were received on 51 of the first-round candidates in the first year. Many of the public comments pointed out errors in security proofs. Some others requested clarifications on definitions and specification details.

A security assessment is the most important and challenging task for the first-round candidates. The security analyses have been conducted from different angles by the various submission teams. Confidence is built on those candidates which are not only proved to be secure, but also continue to stand after withstanding attacks. As could be expected, security flaws or weaknesses were found for some candidates, which may bring the underlying security assumptions into question or fall short of NIST's required security levels. The former can doom an algorithm, while the latter may be fixable through a careful selection of updated parameters and key sizes.

Even though cost and performance were not the primary focus points for the first-round evaluation, the candidates were considered for their feasibility to be used in existing applications. Some of the main features considered include computational efficiency and the memory requirements in each of the operations (key generation, encryption/decryption, signature generation/verification), as well as the size of public keys, ciphertexts, and signatures.

For each of the candidate algorithms, the designers must carefully consider trade-offs between security and performance, which is a difficult decision. One example, which may be of interest for the mathematics community, is among the category of lattice algorithms based on the Learning With Errors (LWE) problem. Using structured lattices defined using cyclotomic rings can improve efficiency, resulting in much smaller public key sizes. However, the Ring-LWE versions of the lattice problems have not be been proven to be equivalent to the generic LWE lattice problems. As a result, some design teams submitted two versions of their algorithm. One is based on the generic LWE, while the other is based on Ring-LWE. Does the extra structure provide avenues for attack? There is much for the research community to explore.

After over a year of analysis and evaluation, in January 2019 NIST announced 26 of the submissions as second-round candidates. The selection of the second-round candidates was based on taking into account the security, cost and performance, and implementation characteristics of each submitted algorithm. At this stage of standardization, algorithm diversity is important to ensure research continues on a variety of fronts since different categories can complement each other. The distribution of the second-round candidates in each category is shown in Table 3.

TABLE 3. Distribution of Second Round Candidates

	Signature	**Encryption/KEM**	**Overall**
Lattice-based	3	9	12
Code-based	0	7	7
Multivariate	4	0	4
Symmetric/Hash-based	2	0	2
Other	0	1	1
Total	9	17	26

5. **Opportunities for Mathematics Researchers.** The NIST post-quantum cryptography standardization process is a multi-year project. The second round is planned to take 12-18 months for the community and submission teams to evaluate and fine tune the candidates. NIST may further narrow down the candidates to

a third round or may select directly among the second-round candidates for standardization. NIST is expected to release the post-quantum cryptography standards sometime around the year 2022 or 2023.

As discussed above, to study quantum-resistant cryptosystems many mathematics problems need to be considered. Submissions to the NIST process came from several different families: lattices, codes, multivariate quadratic equations, isogenies of elliptic curves, and even braid groups. This presents a great opportunity to the mathematics research community. Even though some of these families and their related problems are not new, their properties are not well enough understood yet. In order to have confidence in any cryptosystem, we need to know it has been thoroughly analyzed for potential classical and quantum attacks. These attacks frequently exploit some property or structure of the underlying mathematical framework. For example, isogeny-based post-quantum systems were first proposed using ordinary elliptic curves. After a few years, a quantum attack was discovered which used the fact that the endomorphism ring of ordinary elliptic curves is abelian. Thereafter, isogeny-based schemes began using supersingular elliptic curves (whose endomorphism ring is non-abelian).

There are many unanswered questions pertaining to post-quantum cryptography. When using different algebraic or geometric structures to construct similar cryptosystems, how can their security strength be measured and compared? Can we prove security based on hard, well-studied problems? Why is there a gap between theory and practice in some of the best known attacks (particularly in lattices)? Is it possible to make key sizes of code-based schemes smaller by using more structured codes without compromising security? We will gain more confidence if mathematicians dive deeper into these problems. There is no doubt that a strong mathematical background can help to investigate these problems in a way that people without such a background cannot. Unfortunately, there are not enough mathematicians expert in these areas who are studying the cryptographic implications of their work.

We also note that among the first-round candidates, there were some submissions based on hard problems outside of the three main categories of lattices, codes, and multivariate (see Table 2). These tended to come from areas which have not been very well explored before. Some of these attempts appear to be promising, while others were flawed. Designing a cryptographic algorithm is a very complex venture. It demands knowledge in multiple science and engineering fields. Collaboration is very important. Therefore, this also provides mathematicians an opportunity to work with researchers in other disciplines.

In summary, NIST PQC standardization opens up a broader research space for mathematicians. Researchers are highly encouraged to be involved and to explore new research topics through developing cryptographic standards for the upcoming quantum era. Details about the NIST post-quantum cryptography standardization project can be found at www.nist.gov/pqcrypto.

REFERENCES

[1] S. Aaronson, The limits of quantum computers, *Scientific American* **298**, (2008), 62–69.
[2] L. Adleman, On breaking the titrated Merkle-Hellman public-key cryptosystem, in *Advances in Cryptology: Crypto '82*, Springer (1982), 303–308.
[3] *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*, Federal Register **81**, December 20, 2016. 92787–92788, Available at https://federalregister.gov/a/2016-30615.

[4] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems *J. of Cryptology* **4** (1), (1991), 3–72.

[5] J. Buchmann, E. Dahmen, and M. Szydlo, Hash-based digital signature schemes in: *Post-Quantum Cryptography* (eds. D.J. Bernstein, J. Buchmann, E. Dahmen) Springer, Heidelberg (2009), 35–93.

[6] G. Gentry and M. Szydlo, Cryptanalysis of the revised NTRU signature scheme in *Proceedings of Eurocrypt 2002*, Lect. Notes in Comput. Sci. **2332**, Springer (2002), 299–320.

[7] L. K. Grover, A fast quantum mechanical algorithm for database search, *Proceedings of the 28th Annual ACM Symposium on Theory of Computation*, (1996), 212–219.

[8] J. Hoffstein, J. Pipher, and J.H. Silverman, NTRU: a ring-based public key cryptosystem in *Proceedings of ANTS '98* (ed. J. Buhler), Lect. Notes in Comput. Sci. **423** Springer (1998), 267–288.

[9] R. McEliece, A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report*, Jet Propulsion Laboratory, Pasadena, CA (1978), 42-44. Available at ttp://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.pdf.

[10] D. Moody, *Post-Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions*, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Available at https://csrc.nist.gov/Presentations/2016/Announcement-and-outline-of-NIST-s-Call-for-Submis.

[11] NIST Special Publication (SP) 800-56A Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2018, 141pp. Available from: https://doi.org/10.6028/NIST.SP.800-56Ar3

[12] NIST Special Publication (SP) 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2014, 121pp. Available from: https://doi.org/10.6028/NIST.SP.800-56Br1

[13] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, **26** (5) (1997), 1484–1509. Available at http://dx.doi.org/10.1137/s0036144598347011.

[14] U.S. Department of Commerce, *Data Encryption Standard (DSS)*, Federal Information Processing Standards (FIPS) Publication 46-3, October 1999, 22 pp. Available from: https://csrc.nist.gov/CSRC/media/Publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf.

[15] U.S. Department of Commerce, *Secure Hash Standard (SHS)*, Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, 31 pp. Available from: https://doi.org/10.6028/NIST.FIPS.180-4.

[16] U.S. Department of Commerce, *Digital Signature Standard (DSS)*, Federal Information Processing Standards (FIPS) Publication 186-4, July 2003, 121 pp. Available from: https://doi.org/10.6028/NIST.FIPS.186-4.

[17] U.S. Department of Commerce, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards (FIPS) Publication 197, November 2001, 47 pp. Available from: https://doi.org/10.6028/NIST.FIPS.197.

[18] U.S. Department of Commerce, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards (FIPS) Publication 198-1, July 2008, 7 pp. Available from: https://doi.org/10.6028/NIST.FIPS.198-1.

[19] U.S. Department of Commerce, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, Federal Information Processing Standards (FIPS) Publication 202, August 2015, 29 pp. Available from: https://doi.org/10.6028/NIST.FIPS.202.

[20] 1st NIST PQC Standardization Conference, Ft. Lauderdale, FL, April 11-13, 2018, Available at https://csrc.nist.gov/Events/2018/First-PQC-Standardization-Conference.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: lily.chen@nist.gov
E-mail address: dustin.moody@nist.gov