Trends in Post-Quantum Cryptography— 2020

This report provides an update as of November 2020 on the section titled "1.4.3 Trends in Post-Quantum Cryptography"[*1] in our focused research report in IIR Vol. 31. In the five years since the last report, post-quantum cryptography (PQC) has become so widely known that PQC textbooks[*2] have been published.

2.1 NIST Competition Overview

Last time we reported, we looked at the following four categories of promising algorithms with mathematical backgrounds (IIR Vol. 31, Table 2: Post-Quantum Cryptography Classifications).

- Lattice-based cryptography
- Code-based cryptography
- Multivariate cryptography
- Hash-based signatures

In addition to the above four categories, a cryptosystem known as isogeny-based cryptography also appears as a classification in the latest NIST competition[*3] report. Considerable time was devoted to discussing isogeny-based cryptography at the ECC2018 workshop[*4] held at Osaka University in November 2018, and the elegant figures presented by Chloe Martindale were a pleasure to simply gaze at.

To set up the algorithm in elliptic curve cryptography protocols like ECDH, we create a group structure by defining an additive operation for points on an elliptic curve determined as one of the public parameters and use the characteristics of the elliptic curve discrete logarithm problem. We define a point Q as $Q = kP$, meaning point P added k times. Security in this case relies on the difficulty of finding k given P and $Q = kP$. An isogeny is a type of mapping from one elliptic curve to another, and a key exchange method with a mathematical structure similar to the Diffie-Hellman key exchange algorithm has been proposed on the basis that it is difficult to find a mapping φ given the elliptic curves E and $E' = \varphi(E)$.

Dustin Moody gave a NIST announcement during his invited talk at PQCrypto2016 held in Fukuoka in February 2016, revealing plans for a post-quantum cryptography competition[*5]. The criteria for submissions were finalized at end-2016, and 82 algorithms were submitted by the November 2017 deadline. The submissions were screened, and 69 were selected as first-round candidates[*6]. Following intensive discussion at NIST's First PQC Standardization Conference in April 2018, in January 2019 NIST released NISTIR 8240[*7] and announced that 26 algorithms had advanced to the second round.

In August 2019, NIST held its Second PQC Standardization Conference, co-located with CRYPTO2019, and on July 22, 2020, it announced that seven finalists and eight alternates were advancing to the third round. A detailed status report on the selection process appeared in NISTIR 8309[*8]. Dustin

*1 Internet Infrastructure Review Vol. 31, "1.4.3 Trends in Post-Quantum Cryptography" (https://www.iij.ad.jp/en/dev/iir/031.html).
*2 An example of a post-quantum cryptography textbook in Japanese (https://www.morikita.co.jp/books/book/3503).
*3 NIST Post-Quantum Cryptography (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography).
*4 ECC2018 (https://cy2sec.comm.eng.osaka-u.ac.jp/ecc2018/program.html). Chloe Martindale's presentation slides on CSIDH, CSIDH: An Efficient Post-Quantum Commutative Group Action (https://cy2sec.comm.eng.osaka-u.ac.jp/ecc2018/slide/slide_program/1121-3%20CSIDH%20Martindale.pdf).
*5 Dustin Moody, Post Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions, PQCrypto2016 (https://csrc.nist.gov/presentations/2016/announcement-and-outline-of-nist-s-call-for-submis), (https://www.youtube.com/watch?v=nfLAVybabMs).
*6 Dustin Moody, The ship has sailed: The NIST Post-Quantum Cryptography "Competition", Asiacrypt2017 invited talk (https://csrc.nist.gov/presentations/2017/the-ship-has-sailed-the-nist-post-quantum-cryptog), (https://www.youtube.com/watch?v=3doS6joRYTE).
*7 NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process (https://csrc.nist.gov/publications/detail/nistir/8240/final).
*8 NISTIR 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process (https://csrc.nist.gov/publications/detail/nistir/8309/final).

himself published a blog post in December 2020 giving some background on these developments[*9].

Table 1 is a list of finalists and alternates created from Dustin's latest presentation materials[*10][*11] (alternates are shown in parentheses in red).

Of the seven finalists, three are digital signatures (two of those are lattice cryptography, one is multivariate public key cryptography) and four are key encapsulation mechanisms, or KEMs (three of those are lattice cryptography, one is code-based cryptography). Tweaks to each of the algorithms were allowed at the start of round three, and information on the algorithms and links to their websites appear on the Round 3 page[*12]. PDF documents listing the updates are also available[*13].

The timeline for the competition from here out is as follows. Round 3 (already commenced) is slated to last 12–18 months, at the end of which, NIST will select at most one of the finalists categorized as lattice schemes from the digital signature candidates and, likewise, at most one of the lattice schemes from the KEM candidates. NIST plans to hold a third conference in spring/summer 2021, and it tentatively expects draft standards to be available in 2022–23, and a standard to be published in 2024.

A project called PQCRYPTO was funded under the Horizon 2020 budget[*14]. It is evident from the "D5.2 Standardization: Final report" that PQCRYPTO's contribution to the NIST competition is sizeable. For example, of the 15 algorithms that advanced to Round 3, 11 were PQCRYPTO project submissions.

2.2 Cryptographic Algorithms Published by NIST and Their Impact

NIST has created a range of specifications and guidelines strongly linked to US government procurement requirements. NIST covers an extraordinarily wide range of technological fields, but from what we mainly see, its various guidelines related to information security receive significant attention. The documents on passwords specified in SP 800-63, for example, are read by many engineers and have triggered discussion on how we think about passwords. Fruitful discussion has taken place in Japan, too, regarding the pros and cons of periodically changing passwords and the pros

Table 1: List of Finalists and Alternates

Category/method	Digital signatures	KEM
Lattices	CRYSTALS-DILITHIUM, FALCON	CRYSTALS-KYBER, NTRU, SABER (FrodoKEM, NTRU Prime)
Code-based	None	Classic McEliece (BIKE, HQC)
Multivariate public key	Rainbow (GeMSS)	None
Hash-based signature	(Picnic, SPHINCS+)	N/A
Isogeny	None	(SIKE)

*9 Dustin Moody, The Future Is Now: Spreading the Word About Post-Quantum Cryptography, December 2, 2020 (https://www.nist.gov/blogs/taking-measure/future-now-spreading-word-about-post-quantum-cryptography).
*10 NIST PQC Standardization Update - Round 2 and Beyond, September 23, 2020 (https://csrc.nist.gov/Presentations/2020/pqc-update-round-2-and-beyond).
*11 NIST PQC Standardization Update - Round 2 and Beyond (https://www.nccoe.nist.gov/file/3-pqc-nccoepdf).
*12 Post-Quantum Cryptography Round 3 Submissions (https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions).
*13 History of PQC Standardization Round 3 Updates (https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/history-pqc-round-3-updates.pdf).
*14 PQCRYPTO project (https://pqcrypto.eu.org/), (https://cordis.europa.eu/project/id/645622). D5.2 Standardization: Final report (https://pqcrypto.eu.org/deliverables/d5.2-final.pdf).

and cons of using SMS messages in two-factor or multifactor authentication.

Also, many engineers who use, or who are involved in the use of, cryptographic algorithms know that the NIST publication series FIPS and SP continue to lead the world. While NIST also develops SHA-2, a set of widely used hash functions, suspicions that backdoors might exist given the US government's involvement have been around since DES was developed and published in the 1970s. As such, it is true that similar suspicions regarding the public parameters used in the elliptic curve cryptography method known as NIST curves have recently spurred a preference among some people for cryptographic methods standardized by the IETF as part of a grassroots effort. Yet many of the hash function algorithms implemented in cryptoassets based on blockchain technologies were laid out by NIST. There are cases in which the design and implementation of systems by engineers not well versed in cryptography has led to problems with the survival of the cryptoassets themselves, and it does seem like some people think of SHA-2 as being a secure, well-established technology that has been adequately scrutinized.

2.3 Views on Security in Post-Quantum Cryptography

The security of RSA relies on the difficulty of factoring certain numbers, but anyone can easily factor numbers up to, say, 100 or so (you just need to check divisibility by 2, 3, 5, 7, 11, and 13 for instance). The RSA cryptosystem is based on computational security, so it requires sufficiently large prime numbers to be used securely. The current recommendation is to use a composite number N of at least 1024 bits x 2 = 2048 bits, but consensus on this key length has continued to change with the times. What this tells us is that parameter settings, which rely on the security of the cryptographic algorithm, are of utmost importance. RSA is currently still recognized as secure, but this is because a sufficient key length is maintained. It can only be used securely if correctly implemented on that basis.

The same sort of issues with parameter settings apply to post-quantum cryptography. Even if a cryptosystem itself is thought to be secure, you still need to consider what sort of data should be used in terms of the analog of key length, for example, to ensure security. In this context, key length is an important consideration for cryptographic algorithms, especially the sort of public key cryptographic methods that achieve security through computational complexity currently in use. Similarly, an important issue for post-quantum cryptographic algorithms will be how the various parameters should be set to be secure. So for some categories, cryptanalysis competitions are being held to determine whether the methods are suited to current computing environments, and it is clear in some cases that the sharing of the latest attack methods is something that excites and stimulates the research community.

Competitions dealing with post-quantum cryptosystems classified as multivariate cryptography have been held since 2015. Owing to rapid advances in the research, cryptographic algorithms for which we had assumed some set of parameters was adequate have turned out not to be as secure as we thought in many cases. A presentation by Jintai Ding[*15] at the Second PQC Standardization Conference[*16] co-located with CRYPTO2019, for instance, necessitated a major review of parameters.

*15 Jintai Ding, New Attacks on Lifted Unbalanced Oil Vinegar (https://csrc.nist.gov/Presentations/2019/new-attacks-on-lifted-unbalanced-oil-vinegar).
*16 Second PQC Standardization Conference (https://csrc.nist.gov/events/2019/second-pqc-standardization-conference).

2.4 Bit Security

The cryptographic algorithms widely used today are called classical algorithms, as opposed to post-quantum cryptography. The common way of thinking about security with classical algorithms is that you select parameters to achieve a certain level of bit security. This concept of bit security is easy to understand in the context of symmetric key cryptography and hash functions, and past IIR reports have discussed the compromise of cryptographic algorithms and equivalent security[*17].

For example, the widely used symmetric key cryptographic algorithm AES-128 uses a 128-bit key, and 2128 operations are required to identify the decryption key, so it is said to have 128-bit security. The notion of bit security can also be applied to public key cryptosystems, letting us compare the degree of security offered by cryptographic algorithms based on certain key parameters. NIST publication SP 800-131A[*18] is a well-known source of tables comparing key lengths that is often cited, but what is interesting is that even for the same RSA key length, there is a little variation among different stakeholders' assessments of the level of bit security (see, for example, Table 1 in Section 1.4.1 of IIR Vol. 8).

Past reports on post-quantum cryptography have also contained similar cases in which the strength of an algorithm changes depending on what view the group or organization has formulated. Grover's algorithm, which I discussed in my previous report on post-quantum cryptography, has been shown to reduce the bit security of a symmetric key cryptosystem with n bits of security by half. But there are also reports indicating that some stakeholders have determined that the security of all symmetric key cryptosystems will drop to zero bits. In the case of symmetric key cryptography, the view that the exponent n in 2^n (which indicates how many operations are required for decryption) will fall by half is now widely accepted. Because NIST is running a competition on asymmetric key cryptosystems such as KEMs and digital signatures, symmetric key cryptography does not receive much attention as a post-quantum encryption scheme, but a number of independent research papers with intriguing findings have been published. One, for example, looks at how much of a threat quantum computing poses to the widely used AES[*19]. Based on their analysis, the paper's authors assert that there is a wide security margin in both the classical and quantum computing worlds, but we leave the assessment of this analysis and its prospects up to the reader.

2.5 Quantum Cryptography and Post-Quantum Cryptography

The two terms quantum cryptography and post-quantum cryptography have different meanings and backgrounds, but judging by some mainstream media articles, this seems to be the source of some confusion among the general public. An example in the case of the former is quantum key distribution, or QKD, which is a different concept from post-quantum cryptography. The technical subjects we cover in this report are part of the field known as post-quantum cryptography. We do not discuss technical topics that deal directly with quantum mechanics, such as quantum communication.

*17 For a discussion on the compromise of cryptographic algorithms, bit security, and equivalent security, see IIR Vol. 8 (https://www.iij.ad.jp/en/dev/iir/008.html), "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms".

*18 NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019. (https://doi.org/10.6028/NIST.SP.800-131Ar2).

*19 Xavier Bonnetain et.al, Quantum Security Analysis of AES (https://tosc.iacr.org/index.php/ToSC/article/view/8314). Presented at FSE2020 (https://fse.iacr.org/2020/program.php).

Discussion around post-quantum cryptography focuses on what sort of impact the implementation and widespread availability of quantum computers, assuming this happens, would have on the cryptographic algorithms currently in use. Some readers may therefore be very surprised to learn that post-quantum encryption is already implemented in Web browsers and such[*20]. Reports in the press saying that quantum computers are already in commercial circulation may lead to the misunderstanding that cryptographic algorithms than run on those quantum computers have been implemented. The models we deal with, however, should be understood as modelling attacks on the basis that only attackers with quantum computers have access to the enormous amount of computing power that quantum computing provides, while the vast majority of people are using classical computers.

2.6 What Does Post-Quantum Cryptography Mean?

The definition of post-quantum cryptography is not clear, and it is very difficult to delineate a proposed algorithm as being post-quantum or not, but a decent way to think about it is that post-quantum algorithms are those for which security relies on factors other than the computational security employed by the widespread cryptographic algorithms of the past. That is, we can think of them as replacements for algorithms that are implementable on classical computers.

So even some algorithms proposed way back in the 1970s, for example, are being revisited and featured as post-quantum cryptographic methods.

Meanwhile, research on yet other algorithms has advanced rapidly in the past few years, post-quantum cryptography is becoming a major topic in the cryptographic research community.

Two triggers that drive cryptographic research are the discovery of attacks that make today's commonly used algorithms unusable (i.e., the compromise of cryptographic algorithms), and the prospect of attacks with a large enough impact to render algorithms unusable in the future. An example relevant to the latter is the formulation of a new hash function called SHA-3. NIST selected a proposed algorithm that is internally different from the mathematical structure used in the design of SHA-1 and SHA-2 to become the standard (published as FIPS documents). But almost no progress has been made migrating to SHA-3 and it is believed that SHA-2 can still be safely used. Post-quantum cryptography is also seen as relevant to the latter and is more of an effort to prepare for the future rather than a reaction to algorithms being compromised.

The concept of agility in cryptographic algorithms highlights the importance of having "another card up your sleeve" in terms of cryptographic algorithms designed based on differing ideas and backgrounds, and indeed a whole host of algorithms with various backgrounds are featured in the current efforts to develop post-quantum cryptography. Of them, the lattice-based cryptographic algorithms that have been the subject of research since the 2000s are strong contenders and account for many of the remaining finalists.

*20 qTESLA (https://qtesla.org/) and NewHope (https://www.imperialviolet.org/2018/04/11/pqconftls.html) were not selected for Round 3, whereas SIDH (https://blog.cloudflare.com/introducing-circl/) did make it to Round 3.

2.7 Impact of Post-Quantum Cryptography on Symmetric Key Cryptography and Hash Functions

A look solely at algorithms in the NIST competition seems to indicate that post-quantum cryptography is focused only on public key cryptosystems, but this is not the case in actual practice. Hybrid systems that use, for example, symmetric key encryption along with public key encryption are in use. The digital signature methods use two kinds of algorithms to sign messages with a cryptographic hash function and a public key cryptosystem. The balance between the two algorithms is crucial in these hybrid methods, and you need to consider whether each of the algorithms has n-bit security. As such, we also need to consider the impact of the advent of quantum computers on symmetric key cryptography and cryptographic hash functions. In light of Grover's algorithm, it is known that a symmetric key algorithm with an n-length key has only n/2 bits of security. In specific terms, once quantum computers eventually arrive, using a cryptographic algorithm with 256-bit security only provides the same strength as a classical cryptographic algorithm that uses a 128-bit key[*21].

Next, how should we approach hash functions? Cryptographic hash functions need to have two cryptographic properties. One is collision resistance, and the other is preimage resistance. It is known that on classical computers, hash functions with an output size of n bits have n/2-bit collision resistance and n-bit preimage resistance. Grover's algorithm is the most optimal for the latter, and it is known that the number of operations required for a preimage attack on a hash function with n-bit output falls to $2^{n/2}$.

The number of operations needed to find a collision using a quantum computer using an efficient algorithm called BHT is $2^{n/3}$, but this attack requires $2^{n/3}$ of quantum memory, which is a huge amount that makes the attack unrealistic[*22].

In CRYPTREC Report 2019 (a group of documents summarizing the results of CRYPTREC activity in FY2019)[*23], Akinori Hosoyamada's commentary says that the CNS algorithm[*24] is the one most realistically likely to have an impact and reports that this algorithm can find collisions in $2^{2n/5}$ operations. For example, the SHA-256 algorithm has 128 bits of security (in terms of collision resistance), so even attacking it using the CNS algorithm would require over 2^{100} operations, and Hosoyamada therefore concludes that it probably does not pose a realistic threat. Hence, it is thought that the advent of quantum computers should have less of an impact on symmetric key cryptography and hash functions than it does on public key cryptography. In the sense that one can make ready by using algorithms already published and put into widespread use, there is not much to do in the way of preparations at this point.

*21 Internet Infrastructure Review (IIR) Vol. 31, 1.4.3 Trends in Post-Quantum Cryptography (https://www.iij.ad.jp/en/dev/iir/031.html).
*22 Gilles Brassard et al., Quantum cryptanalysis of hash and claw-free functions. SIGACT News 28 (2): 14–19, 1997.
*23 Akinori Hosoyamada, Investigation and Assessment of the Impact of Quantum Computers on Symmetric Key Cryptography, CRYPTREC EX-2901-2019, Jan. 2020. (https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf, in Japanese).
*24 Andre Chailloux et al., An efficient quantum collision search algorithm and implications on symmetric cryptography, LNCS10625, pp.211–240, Asiacrypt2017, 2017.

2.8 CRYPTREC's View on the Threat of Quantum Computers

In February 2020, the CRYPTREC Cryptographic Technology Evaluation Committee issued an alert[*25] that offered CRYPTREC's response from a technical perspective to a paper that had, at the time, recently appeared in Nature claiming to have realized quantum supremacy on a quantum computer[*26]. The alert reported that although the paper had raised concerns that the security of widely used public key cryptographic methods could be greatly diminished, the likelihood of the cryptographic algorithms in CRYPTREC's cipher list being compromised is low. The basis for this assertion was that the paper in question assumes an ideal environment with zero quantum errors, and that another paper[*27] claiming that RSA integers can be factored in 8 hours estimates that 20 million qubits would be needed, a situation far removed from current progress in the implementation of quantum computers.

CRYPTREC's rationale for issuing the alert was that it needed to "Release accurate, highly trustworthy information as a means of preventing overreactions" under item B in its communications workflow that applies when information on vulnerabilities in cryptographic algorithms is detected. Refer to Chapter 1 of CRYPTREC Report 2019 for background information and details of the communications workflow.

2.9 Dialog with People at NIST

At a workshop[*28] co-located with EUROCRYPT2016, I had the pleasure of talking with NIST's Lily Chen about policies on cryptography including the post-quantum variety. I pointed out that NIST has two different cryptography policy directions: post-quantum cryptography and lightweight cryptography. At the time, I only envisioned the post-quantum response for symmetric key cryptography would entail extending the life of the technology by, for example, doubling key lengths. I asked whether NIST would be looking at developing new algorithms, like AES-512 for instance, or turning to, say, Triple AES (using a three-key bundle like Triple DES). Her answer was that we already have AES-256, which was secure at the time and will provide 128-bit security with key lengths available in 2030 and beyond, so even AES-256 will provide sufficient resistance to quantum computers.

I also hadn't imagined the introduction of symmetric key cryptographic methods with new backgrounds, like in public key cryptography, but at FSE2020, there was actually a presentation about Saturnin, a post-quantum symmetric key cryptosystem[*29]. Saturnin is both a lightweight and post-quantum cryptographic suite of algorithms. A NIST competition aimed at standardizing lightweight cryptography is also underway. Such algorithms are called lightweight as they are aimed at devices with little computing power,

*25 CRYPTREC Cryptographic Technology Evaluation Committee, The impact of current quantum computers on the security of cryptographic technologies, Feb. 17, 2020, CRYPTREC ER-0001-2019 (https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html, in Japanese).

*26 Frank Arute et al., Quantum supremacy using a programmable superconducting processor, Nature 574, pp. 505–510, 23 October 2019. (https://doi.org/10.1038/s41586-019-1666-5).

*27 Craig Gidney et. al, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (https://arxiv.org/abs/1905.09749).

*28 9th International View of the State-of-the-Art of Cryptography and Security and its Use in Practice (https://www.iacr.org/conferences/eurocrypt2016/Vienna-May13-2016.pdf).

*29 Anne Canteaut et.al., Saturnin: a suite of lightweight symmetric algorithms for post-quantum security, FSE2020 (https://iacr.org/cryptodb/data/paper.php?pubkey=30514). Presented at FSE2020 (https://fse.iacr.org/2020/program.php). Saturnin project (https://project.inria.fr/saturnin/).

such as IoT devices. Key lengths of around 80 bits are envisioned, and security is weaker than with commonly used algorithms. CRYPTREC also ran a lightweight cryptography working group from FY2013 through FY2016, and in June 2017 it published the CRYPTREC Cryptographic Technology Guideline - Lightweight Cryptography*30 with the objective of supporting the appropriate use of lightweight cryptography. Holding separate competitions for lightweight cryptography, like those for lattice-based methods and such, provide an opportunity to test whether your own method is secure, and this is one area of research that I am personally very excited about seeing future developments in.

Cryptographic algorithms are being standardized for various use scenarios. As discussed above, the advent of quantum computers will not immediately have an impact, but you can keep up with the latest trends via the CRYPTREC website, so I encourage you to take a look.

Yuji Suga
Senior Engineer, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ.
Dr. Suga has been in his current position since July 2008. He is engaged in investigation and research activities related to cryptography and information security as a whole. He is a member of the CRYPTREC Cryptographic Technology Promotion Committee. He is also secretariat of the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium (CELLOS); secretary of the Information Processing Society of Japan's Computer Security Group (CSEC); IWSEC2021 General co-chair; AsiaCCS'22 General co-chair; Cryptoassets Governance Task Force (CGTF) Security Working Group member; APSIPA Multimedia Security and Forensics Technical Committee member; and BGIN (Blockchain Governance Initiative Network) co-initial contributor.

*30 CRYPTREC Lightweight Cryptography Working Group, CRYPTREC Cryptographic Technology Guideline - Lightweight Cryptography (https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016en.pdf). CRYPTREC Symposium 2017, Introduction to the Lightweight Cryptography Guideline (https://www.cryptrec.go.jp/symposium/20171218_cryptrec-lw.pdf, in Japanese).