Cryptography is the study of methods of secure communication, and its applications are ubiquitous in everyday life. Results from cryptography naturally enter policy discussions through issues of national defense. Despite its prevalence and importance, modern cryptography can be difficult for general audiences to understand because it is deeply rooted in technical ideas from theoretical and applied sciences.

The convergence of highly technical topics from cryptography with important policy objectives, such as cybersecurity, creates a need to understand recent developments in cryptography at a granular level. The National Institute of Standards and Technology (NIST) has predicted that advancements in quantum computing will threaten certain communication technologies by overcoming modern protections against eavesdropping and unwanted viewing of secured messages (L. Chen et al., 2016). Determining the scope and severity of the threat is a problem for a broad audience of stakeholders.
The goal of this Perspective is to provide a focused view of the search for quantum-resistant cryptographic methods. We explain different avenues for securing communications from quantum attacks and argue that cryptographic research in the quantum era will benefit from open access to results. We conclude by identifying activities that policymakers can consider to positively influence the outcome of the pending post-quantum cryptography (PQC) migration.

Quantum Computing’s Near-Term Effects on Cryptography

Public-Key Cryptography

For most of history, cryptographic methods depended on prearranged, shared secrets for their security. The famous Caesar cipher was used to encrypt messages by shifting letters in words by a uniform distance in the alphabet, and anyone who knew the amount of shift could easily decrypt the message (Hoffstein, Pipher, and Silverman, 2008). The shift is an example of a key, or information that is used to protect and recover messages.

The discovery of public-key cryptography (PKC) marks a significant milestone in the development of cryptography because it introduced a new paradigm for securely sending information. The concept was first defined in a paper by Whitfield Diffie and Martin Hellman in 1976, although it was discovered independently around the same time by James Ellis in 1969 and Ralph Merkle in 1974. The characterizing feature of PKC is the use of public and private keys. In its simplest form, a public-key scheme specifies how a user’s public and private keys are combined to allow anyone in possession of the public key to securely send messages to the user. Unlike prior cryptographic schemes, PKC does not require a secure communication medium—public keys and messages can be exchanged, for example, over an internet connection. When properly designed, PKC methods are broadly resistant to modern computer analysis. In practice, distinct parties maintain their own private and public keys, and the resulting system of keys allows each user to securely authenticate identities and establish secure channels of communication.

In a PKC scheme, the method of combining public and private keys determines its theoretical level of security. Ideally, the method is designed to make decryption of encrypted messages infeasible without the private key. Most modern PKC methods are based on two mathematical procedures: the factorization of integers, and the computation of an object called the discrete logarithm. In cryptography, these procedures are often posed as problems. The former procedure challenges a would-be attacker to

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIKE</td>
<td>Bit Flipping Key Encapsulation</td>
</tr>
<tr>
<td>FDH</td>
<td>Full Domain Hash</td>
</tr>
<tr>
<td>HSRD</td>
<td>RAND Homeland Security Research Division</td>
</tr>
<tr>
<td>LWE</td>
<td>learning with errors</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>PKC</td>
<td>public-key cryptography</td>
</tr>
<tr>
<td>PQC</td>
<td>post-quantum cryptography</td>
</tr>
<tr>
<td>PSS</td>
<td>Probabilistic Signature Scheme</td>
</tr>
<tr>
<td>SIKE</td>
<td>Supersingular Isogeny Key Encapsulation</td>
</tr>
<tr>
<td>TLS</td>
<td>transport layer security</td>
</tr>
</tbody>
</table>
find an algorithm (i.e., instructions for a computer) that, given any whole number, determines the complete list of its smallest factors. A method based on factorization would convert the difficulty of solving the factorization problem into difficulty of decrypting messages without prior knowledge of the private key.

The Need for Post-Quantum Cryptography

Quantum computers are theoretical devices that leverage quantum mechanical properties of matter to accomplish computing tasks. Since they were first proposed in a thought experiment about simulating physical systems (Feynman, 1982), quantum computers have become a focal point of intense research. Researchers at the National Academies of Sciences, Engineering, and Medicine (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing, 2019) predicted that the successful realization of useful quantum computers would occur no sooner than 2026; a 2022 report by the Global Risk Institute (Mosca and Piani, 2022) states that the development of a useful quantum computer by 2026 is very unlikely. Despite this, quantum computing researchers have already identified applications that have the potential for revolutionary breakthroughs in both basic and applied sciences.

Although current computing technology cannot efficiently solve either the factorization problem or the discrete logarithm problem, it is widely believed that advanced quantum computers will not have this limitation. In 1994, Peter Shor constructed novel solutions to both factorization and discrete logarithm problems and gave mathematical proof that these solutions can run as efficient algorithms on an advanced quantum computer (Shor, 1994). In the literature, both solutions are referred to as Shor’s algorithm. Although Shor’s discoveries do not threaten all encryption methods, they do threaten PKC, and engineering progress in creating advanced quantum computers has spurred a complementary effort to create quantum-resistant communication systems.

These efforts fall into two categories. Quantum cryptography uses quantum physics to implement cryptographic schemes. Recent years have seen breakthroughs in quantum cryptography, such as the realization of small-scale, device-independent quantum key–distribution systems (Liu et al., 2022; Nadlinger et al., 2022; Zhang et al., 2022) and first steps toward large-scale quantum networks (Y. Chen et al., 2021). However, quantum cryptographic methods are experimental and require specialized infrastructure to implement, and their security in real-life applications is untested. Additionally, as of 2020, the National Security Agency (NSA) did not recommend quantum cryptography as a protection for national security systems against quantum computing (NSA, 2020). Similar positions have been stated by the United Kingdom’s National Cyber Security Centre (2020) and France’s Agence nationale de la sécurité des systèmes d’information (undated). For these and other reasons, it is unlikely that quantum cryptography will see widespread use in the near future.

In contrast, PQC, the topic of this Perspective, is the study of cryptographic methods that can be implemented on current computing systems. PQC algorithms use mathematical protections to safeguard against both quantum and nonquantum computing threats. Generally, two important activities of PQC are finding problems that cannot be solved efficiently, even with the aid of quantum
computers, and designing cryptographic algorithms that exploit these problems to create quantum-resistant communication channels.

The present goal of PQC is to enable a transition away from vulnerable public-key methods toward public-key methods that cannot be broken easily by quantum or nonquantum algorithms. Replacing vulnerable computer systems to protect information against quantum attacks is a strategic objective in the U.S. National Cybersecurity Strategy (White House, 2023), and preparations for this PQC migration have already begun. Notably, in 2016, NIST opened a public call for quantum-resistant algorithms to begin developing standards for PQC. Part of the standardization process is screening candidates for security and performance, with competitive candidates advancing through rounds of evaluations (Computer Security Resource Center, 2016). At the time of this writing in the summer of 2023, NIST has selected four candidates for standardization from its third round of evaluations and promoted several of the remaining candidates for an ongoing fourth round.

**Two Influential Factors in Algorithm Development for Post-Quantum Computing**

In this section, we highlight two factors that influence PQC algorithm development: choice of methods and availability of theoretical security guarantees. We use the two factors highlighted here to motivate discussions in the next section about transparent algorithm development and cryptographically agile implementation of PQC. An important caveat is that this Perspective is far from comprehensive—we do not, for example, discuss the important issues of cost, algorithm performance, and intellectual property, which are significant criteria for NIST’s ongoing effort to create PQC standards. (Computer Security Resource Center, 2016).

**Factor 1: Choice of Methods**

PQC algorithms are characterized by the methods they employ to encrypt messages. Knowing the mathematical basis of a PQC algorithm is important because it largely determines the theoretical security of the algorithm. Currently, there are several distinct proposals for securing PQC algorithms. However, the NIST evaluation results show a preference for a single category of algorithms whose security is based on mathematical objects called **lattices**. In the future, selective pressures, such as research preferences or successful attacks on developing security systems, might reduce the number of distinct methods in practice. Whether this outcome would have a significant effect on the security of communication systems is an important open question for policymakers and industry stakeholders to consider.

Most PQC public-key algorithms base their security on one or more of the following types of problems (Bernstein, Buchmann, and Dahmén, 2009):

- lattice problems
- code-based problems
- multivariate polynomial root-finding
- hash-based problems
- elliptic-curve isogenies.
For example, an algorithm that uses lattice problems is a lattice-based algorithm. Two algorithms that use methods from the same family of problems can still have very different behaviors with respect to security and functionality.

Public-key PQC algorithms are one of many types of building blocks for a cryptosystem (a collection of algorithms whose combined use establishes a technique for encrypting and reading messages). The different methods used by a cryptosystem describe how the system achieves its security. A cryptographic protocol specifies how to implement cryptosystems and other algorithms to create secure channels for communication. In the next section, we discuss an important example of a cryptographic protocol called the transport layer security (TLS) protocol, which uses both public keys and other methods to protect internet communications.

As of this writing in the summer of 2023, methods from each of the five types of problems listed above are active areas of PQC research, but we found an emerging trend toward lattice-based methods. In the table are our findings from technical documents available on the NIST PQC website to classify the third-round candidates by method and identify examples of PQC algorithms in each class (Alagic et al., 2022). NIST planned to hold another call for proposals, ending in June 2023, for digital signature algorithms, with an emphasis on methods that are not lattice-based (Computer Security Resource Center, 2022).

Classification can be a nontrivial task. An example that illustrates this is Kyber, one of the algorithms that NIST chose for standardization in 2022. The security of the Kyber algorithm is backed by a family of problems known as learning with errors (LWE) (Avanzi et al., 2021). However, to fit in the classification of our table, it was ultimately identified as a lattice-based algorithm through a sequence of research papers beginning with Oded Regev’s pioneering work on LWE (Regev, 2009).

Some of NIST’s third-round candidate algorithms were later found to be flawed. Castryck and Decru (2023) demonstrated an attack on the third-round candidate SIKE. Their result is notable partly because it relies on an algebro-geometric theorem by Kani which had been proven without cryptographic motivations (Kani, 1997). Rainbow, another third-round finalist, was broken by Beullens in 2022. This attack (Beullens, 2022) is notable because Rainbow’s security had been investigated in a series of attacks and improvements, from its introduction in 2005 to its last update in 2020, which claimed to present a proof of secu-

<table>
<thead>
<tr>
<th>Problem Type</th>
<th>Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice problem</td>
<td>Kyber, a Dilithium, a NTRU, NTRU Prime, Saber, Falcon, a FrodoKEM</td>
</tr>
<tr>
<td>Code-based problem</td>
<td>Classic McEliece, BIKE, Hamming Quasi-Cyclic (HQC)</td>
</tr>
<tr>
<td>Multivariate polynomial root-finding</td>
<td>Rainbow, Great Multivariate Short Signature (GeMSS)</td>
</tr>
<tr>
<td>Hash-based problem</td>
<td>SPHINCS+ a</td>
</tr>
<tr>
<td>Elliptic-curve isogeny</td>
<td>SIKE</td>
</tr>
<tr>
<td>Other</td>
<td>Picnic</td>
</tr>
</tbody>
</table>

NOTES: BIKE = Bit Flipping Key Encapsulation; SIKE = Supersingular Isogeny Key Encapsulation.
a Selected in 2022 for standardization at the end of the third round.
rity for the submitted version of Rainbow (Alagic et al., 2022; Ding and Schmidt, 2005).

It is uncertain what effect these attacks will have on the future development of isogeny-based and multivariate-based algorithms. For example, Castryck and Decru (2023) concluded that SIKE appears fully broken and unsuitable for secure use. We can imagine that SIKE’s failure could discourage further development or adoption of isogeny-based algorithms out of concern that isogeny-based problems would be vulnerable to similar attacks, regardless of whether the Castryck–Decru result can be generalized to apply to a broader scope of algorithms.

**Factor 2: Availability of Theoretical Security Guarantees**

Lattice-based PQC algorithms have a special role in the search for quantum-resistant schemes because of the cryptographic community’s confidence in certain lattice-based algorithms’ qualitative security guarantees against attack. The guarantees are based on a form of mathematical analysis called *reduction.* These proofs give qualitative metrics of security for the constructed algorithms, allowing coarse-grain comparisons between them. They also provide standards to which the algorithms can be fine-tuned, adding a necessary, quantitative measure of security. Plainly put, a reduction is a relationship between two problems in which an assumed solution of one problem implies the existence of a solution to the other. In cryptography, one use of a reduction is to derive constraints on the assumed solution, which plays the role of the would-be attack on a cryptosystem. Ideally, a reduction reveals that a realistic attack on the target cryptosystem would be difficult, if not impossible, to find.

Reductions in PQC algorithms are an active topic of research. Tracking developments in this area is important even outside the context of cryptographic analysis because reduction results shape research priorities and preferences for algorithms. One view of this process is that reductions define a constructive paradigm for PQC algorithm development by giving a sense of what a “natural” cryptosystem is and setting the bar for what cryptographic constructions should hope to achieve (Damgård, 2007).

On one hand, the results of reductions are highly technical and abstract. An application of reduction must be scrutinized at the rigorous level of proofs to make sure it is correctly used, and even then, its impact can be qualified. Alkadri et al. (2017) observed that reductions had had less of a practical impact on security analysis for lattice-based algorithms than parameter optimization (i.e., the empirical selection of algorithm settings that offer security against best-known methods of attack) had.

On the other hand, a qualitative security guarantee is valuable partly because it implies a robust level of security that can be tested through analysis and trial. For example, the discovery of particularly strong reductions for lattice problems have put a spotlight on lattice research, and this research has led to “credible estimates” of the security of lattice-based cryptosystems (Computer Security Resource Center, 2022).

For the remainder of this discussion, we continue our description of lattice-based algorithms by describing recent developments in reductions and security guarantees. Our goal is to explain why certain lattice-based algorithms are
thought to be secure and why reductions will continue to be an active research topic for PQC in the future.

Regev’s work on LWE supplied a proof that efficient solutions of certain LWE problems can be converted into relatively efficient solutions for certain lattice problems known generally as shortest-vector problems (SVPs). Two types of shortest-vector problems, gap SVP (GapSVP) and shortest independent vector problem (SIVP), reduce to LWE (Regev, 2010); because there is evidence that instances of GapSVP and SIVP are difficult to solve (Peikert, 2016), efficient solutions of the highlighted LWE problems are likely difficult to find. This implies that successful attacks on LWE are accordingly difficult to construct. The reduction that underlies the Kyber algorithm comes from work by Langlois and Stehlé (2015) and earlier work by Lyubashevsky, Peikert, and Regev (2013).

Although reductions of lattice problems are generally accepted as theoretically valid, recent works to quantify the real-life applicability of reductions in lattice-based schemes have been controversial. One interesting area of investigation is so-called tightness gaps in reduction. To illustrate the concern, we provide this example. Suppose that there are two problems, problems A and B, and A reduces to B. Given a solution $S$ to problem B, the reduction produces a solution $S'$ to problem A. If the cost to implement solution $S'$, quantified in terms of maximal computation time and probability of success, is comparable to the cost to implement $S$, we say that the reduction is tight. Otherwise, the relative difficulty of implementing $S'$ might not translate into a realistic constraint on the difficulty of implementing $S$. In other words, a sufficiently large tightness gap might still allow for an efficient solution to problem B.

The literature on tightness gaps for reductions in lattice-based algorithms reflects the current state of uncertainty. Koblitz et al. (2022) presented an analysis of the Lyubashevsky–Peikert–Regev reduction, claiming that its loose tightness gap and other issues nullify any derived security guarantee. Such claims argue directly against analyses that conclude that cryptosystems based on formulations of LWE, such as Peikert (2009) and (Stehlé and Steinfeld (2011), are provably secure up to the difficulty of standard lattice problems.

Historically, concerns about tightness have been well-founded, and resolving these concerns has led to improved security guarantees. One example comes from methods to securely send and authenticate a digital signature (data that certify a message with information about the identity of the sender and intactness of the message). In the 1990s, Bellare and Rogaway introduced two closely related algorithms, the Full Domain Hash (FDH) and the Probabilistic Signature Scheme (PSS), which have been widely used to implement digital signature schemes. In 1996, Bellare and Rogaway proved security guarantees for FDH and PSS, converting the difficulty of integer factorization into upper bounds on the probability that either scheme can be broken in a given amount of time (Bellare and Rogaway, 1996). As Bellare and Rogaway acknowledged in their 1996 paper, their reduction for FDH was not tight, and their open question about the security of FDH instigated a chain of research that has clarified comparisons between FDH and PSS and improved the security of digital signature schemes that rely on them.

Last, reduction arguments depend on a theoretical understanding of the difficulty of the reduced problem. The study of computational difficulty is called complexity
theory, and the most famous open problem from complexity theory, known as P versus NP, has been unsolved for more than 50 years. Its answer would have direct and possibly negative consequences for security analyses, such as reduction; efforts to resolve P versus NP will certainly continue independently of the status of PQC.

Supporting the Future Effectiveness of Post-Quantum Cryptography

We argue that transparent development contributes to the security of PQC cryptosystems. Trends in research and literature point to PQC algorithms being implemented in the near future, which suggests an opportunity to create cryptographically agile PQC protocols. In this section, we consider future PQC algorithm development and discuss activities that support the end goals of PQC migration.

Benefits of Transparent Development in Post-Quantum Cryptography

At its present state, cryptographic activity around PQC algorithms shares similarities with basic and applied research. The methods of PQC are based in mathematics, and a notable part of the activity aims to produce new theoretical results. Activity in specific research areas, such as reduction and tightness analysis, and in broad areas, such as algebraic geometry, will continue to produce the cryptographic ability and diversity in algorithms necessary to mitigate risks from novel attacks and technologies. The similarity is also reflected in the places of activity. All 15 of the third-round candidates were developed by teams affiliated with universities.

Like the results of research, the specifications of PQC algorithms are often published and distributed widely; one of the minimal acceptability requirements for the NIST PQC standardization call was public disclosure of algorithms, allowing reasonable public review of any candidate. One important reason for wide distribution is the principle of open cryptography—that transparent development of algorithms is more effective in creating secure cryptosystems than development done in secret is. The cryptographic community is more willing to adopt methods that have been transparently vetted because, otherwise, algorithms are black boxes and their security is unverifiable.

For example, initial concerns about the opaque development of NIST standards for a random number generator called Dual_EC_DRBG included suggestions of insecurity (Brown and Gjøsteen, 2007) and claims of intentionally placed weak points in algorithm design (Shumow and Ferguson, 2007). The algorithm was widely shunned by the cryptographic community because the algorithm’s security was not publicly verifiable (Schneier, 2007). By the time NIST removed Dual_EC_DRBG from its standards in 2014, it was clear that NSA had obscured the development of Dual_EC_DRBG and used the secrecy to deliberately introduce weaknesses—the agency had planned to use these weaknesses to bypass encryption methods (Kostyuk and Landau, 2022). Kostyuk and Landau observed that NIST, which had historically played a prominent and international role in standardizing cryptographic algorithms, retained the trust of the cryptographic community through this incident partly because of its long-standing practice of transparent development.
Without transparent development and open access to PQC research, there is a risk of using technology that has not been sufficiently vetted to protect the information infrastructure.

Even the well-intentioned idea of withholding information about vulnerabilities to avoid damage to cybersecurity, as found in Bellovin’s (1995) delayed analysis of weaknesses in the early internet’s domain name system, has fallen out of favor and been replaced by principles of open analysis (Bellovin and Bush, 2002).

Despite high-profile cases, such as Dual_EC_DRBG, it is difficult to argue definitively that openly developed cryptosystems generally fare better than secretly developed cryptosystems because the latter are, by design, inscrutable. For example, there is no way to know from public information whether the classified suite A set of cryptographic algorithms maintained by NSA for government use (Committee on National Security Systems, 2010) is any stronger or weaker than its publicly available suite.

However, we conjecture that the process of open development is more robust than secret development when the methods involved are relatively new or untested. To support this conjecture, we note the example of the Clipper chip. In 1993, the U.S. federal government announced a plan to widely implement a deliberately weakened cryptosystem, which would allow a novel eavesdropping feature: It would permit federal law enforcement to access encrypted messages in cases of crime or threat to national security (Markoff, 1993). The design of the cryptosystem and its implementation on Clipper chips were, for the most part, classified. When NSA made some aspects of the eavesdropping algorithm available to the public, a researcher at AT&T Bell Laboratories quickly demonstrated flaws that led some to question the functionality of the feature (Blaze, 1994). The cryptosystem was ultimately abandoned after subsequent research showed that the proposed eavesdropping algorithm could “jeopardize the proper operation, underlying confidentiality, and ultimate security of encryption systems” (Abelson et al., 1997, p. 10).

Presently, PQC development involves cryptographic novelty. Lattice-based algorithms have trended toward mathematical sophistication (e.g., choosing LWE formulations that involve objects with more structure than originally assumed in Regev’s seminal paper). And reductions and tightness arguments are, in the end, mathematical proofs that are attempting to push security boundaries beyond what is already known. The standard for verification of mathematical results is peer review, which requires open access to details. Without transparent development and open access to PQC research, there is a risk of using
technology that has not been sufficiently vetted to protect the information infrastructure.

Implementation of Post-Quantum Cryptography in Communication Protocols

Unlike quantum cryptography, PQC produces algorithms for existing computer systems. A combination of confidence in theoretical security guarantees and progress in NIST’s PQC standardization process has already prompted several industry experiments with implementation. These experiments provide a glimpse at how industry stakeholders might integrate PQC algorithms into ordinary use and handle future migratory pressure. Notable examples involve the TLS protocol, which is a cornerstone of modern secure messaging and data transmission for the internet.

The TLS protocol has a wide variety of applications centered on securing internet communications, and it is commonly used to negotiate preliminary agreements between users that authenticate communicating parties and share cryptographic information before encrypted messages can be securely exchanged. This preliminary step is called the handshake, and, although the TLS protocol offers several methods to shake hands, the majority of these methods are based on PKC and will need to be replaced during PQC migration. The redundance of handshake methods reflects a modular design philosophy that emphasizes the ability to slot new public-key methods into the protocol without the need for extensive revisions to the protocol itself (Dierks and Rescorla, 2008).

TLS protocols that incorporate PQC algorithms are already in development today (Celi et al., 2021). And industry experiments with post-quantum TLS protocols had begun even before NIST announced its first selections for standardization in 2022. In 2019, technology companies Cloudflare and Google tested implementations of SIKE and a lattice-based algorithm called HRSS, measuring performance of roughly 10 million uses of an experimental TLS protocol over 53 days (Kwiatkowski and Valenta, 2019). In 2019, Amazon Web Services, a cloud computing service, created a TLS protocol that used SIKE and BIKE (Hopkins, 2019) and later Kyber (Weibel, 2023); a test of the latter implementation measured performance over 2,000 TLS handshakes between Amazon Web Services computing systems.

There is a realistic possibility that, as NIST's standardization process concludes and internet standards respond to the introduction of mature PQC algorithms, there will be an increase in the use of hybrid TLS protocols that combine post-quantum and classical methods, creating a wide surface for algorithmic variation. However, important technical questions about the transition, including concerns about computational performance (Schwabe, Stebila, and Wiggers, 2021) and software incompatibilities (Cimpanu, 2021), have not been resolved and stand in the way of, for example, a capable post-quantum TLS protocol.

Addressing a Problem of Cryptographic Agility

Implementations of PQC should be able to respond to sudden and effective breaks of algorithms in their cryptographic suites, especially during the early deployments of PQC algorithms and the uncertain years that will surround the creation of the first advanced quantum computer. Efforts to preemptively prepare for certain events, such as
the attack on SIKE, address important concerns related to cryptographic agility. One important aspect of cryptographic agility is the ability to introduce, maintain, replace, and combine use of algorithms without significant changes to the overall infrastructure of the information system (Barker, Polk, and Souppaya, 2021).

Identifying obstacles to cryptographic agility is important for practical reasons. A cryptographically rigid protocol that depends narrowly on one method, for example, would not be able to easily or quickly adapt to the discovery of an efficient attack, thereby prolonging the time during which the attack could cause damage.

As we have shown with examples of TLS protocols, one obstacle is the technical difficulty of implementing PQC algorithms in an agile way. Besides implementation, protocol agility is also constrained by the availability and proper adoption of enough secure methods. Although the recent need for PQC migration has raised interest in alternative cryptosystems, it is unclear whether standardization and adoption pressures will select only a few methods for use in the future. An overwhelming preference for one or two methods could preclude research and development for other methods, resulting in a limited availability of mature PQC algorithms. Alternatively, many mature PQC algorithms might be available for use, but, in practice, users might choose to deploy them in protocols in unvaried ways. As computer systems are built and updated around these conventions, protocols could become inflexible through a process known as ossification (Vermeer and Peet, 2020). In any case, the outcome would be a constraint on the ability of some protocols, such as TLS, to effectively exchange insecure algorithms for secure ones.

This outcome is potentially problematic. In the future, a break in a PQC cryptosystem comparable to Shor’s algorithm might not be accompanied by decades of preparatory time—much like happened with the comparatively late and sudden break of SIKE. The only mitigating factor in this case would be a diversity of cryptographic algorithms that would allow infrastructure to quickly and effectively swap in an algorithm that could resist this hypothetical attack.

The pending migration caused by Shor’s algorithm presents a unique opportunity to codify new mathematical frameworks, such as lattice-based cryptography, as the foundations of post-quantum cryptosystems. To support this goal, we identify the following impactful activities that can be affected at the level of policy:

- **transparent development and standardization of PQC algorithms**: Many relevant methods required to develop secure PQC algorithms come from applied and theoretical mathematics. These mathematical methods require peer review and cryptographic community input in order to offer both quantitative and qualitative security guarantees. Restrictions on open access of research or standards could lead to improper use of mathematical results, harming cryptographic security in the long run.
- **cryptographically agile implementation**: As companies and other stakeholders implement the first PQC migrations in their communication systems, there is an opportunity to prioritize protocols that are cryptographically agile and to take advantage of the present diversity of cryptographic frameworks. Standards and requirements that emphasize agile implementation would help prepare for future
migrations by reducing pressure to consolidate the available number of secure cryptosystems.

Policies that encourage these activities above will support the future effectiveness of PQC by preparing for sudden and effective breaks of algorithms in cryptographic suites. This technical responsiveness to unforeseen events is one of many capabilities that will determine PQC’s success in creating a secure post-quantum environment for communication. With proper consideration of points like the ones raised in this Perspective, PQC will pave the way for the safe adoption of revolutionary quantum computing technologies whenever they are deployed.

Notes

1 No publicly available document resulted from Ellis’s work.

2 More precisely known as prime factors. Learning all of the factors of a whole number requires knowing only its prime factors.

3 See Boneh and Venkatesan (1998) for a discussion on the necessity of solving the integer factorization problem to break the Rivest–Shamir–Adleman algorithm.

4 The Global Risk Institute authors concluded this through a survey of 46 quantum computing experts, finding that “most experts (25/46) judged that the threat to current public-key cryptosystems in the next 5 years is ‘<1% likely’” (Mosca and Piani, 2022, p. 26). For a full description of likelihoods, see Mosca and Piani, 2022.

5 Although quantum algorithms are technically able to break widely used PKC schemes, the energy cost of running algorithms on capable hardware might limit the applicability of advanced quantum computers. See Parker and Vermeer (2023) for a discussion of energy cost obstructions to breaking public-key encryption.

6 Also known as quantum-resistant cryptography.

7 NSA expects to approve a selection of lattice-based algorithms from NIST’s evaluations for use in national security systems (NSA, undated).

8 Not all lattice-based algorithms derive their security from LWE problems. A notable example is the collection of lattice-based algorithms which comprise the NTRU cryptosystem (Hoffstein, Pipher, and Silverman, 1998). However, interest in provable security motivated the creation of a variant of NTRU which can use a LWE problem to provide a theoretical security guarantee—see Stehlé and Steinfeld (2011).

9 Not to be confused with the mathematical technique of lattice reduction.

10 Damgård noted that “naturality” of a cryptosystem is inherently subjective and states that the “only reasonable approach [to algorithm design] is to construct cryptographic systems with the objective of being able to give security reductions for them” (Damgård, 2007, p. 4).

11 Although we focus on LWE because of its relevance to our discussion of Kyber, the study of reductions of lattice problems for cryptography was initiated by Ajtai (1996).
Bellovin delayed the publication of his 1995 report on early internet weaknesses because he found a “serious vulnerability for which there was no feasible fix.” See the epilogue of Bellovin (1995).

References


Agence national de la sécurité des systèmes d’information, “Should Quantum Key Distribution Be Used for Secure Communications?” webpage, undated. As of July 7, 2023: https://www.ssi.gouv.fr/publication/should-quantum-key-distribution-be-used-for-secure-communications/


Koblitz, Neal, Subhabrata Samajder, Palash Sarkar, and Subhadip Singha, “Concrete Analysis of Approximate Ideal–SIVP to Decision Ring–LWE Reduction,” *Advances in Mathematics of Communications*, early access, October 2022.


Merkle, Ralph, “Project Proposal,” homework for Computer Science 244, Fall 1974.


NSA—See National Security Agency/Central Security Service.


About This Perspective

Advanced quantum devices have the potential to break existing protections for communication technologies. This Perspective provides a focused view of the search for novel protections for computer systems through the field of post-quantum cryptography. The authors identify two factors that affect the development of quantum-resistant algorithms before discussing activities that can positively influence the outcome of the pending migration away from vulnerable encryption standards and protocols. The primary audience of this Perspective is U.S. government policymakers who work on issues of cybersecurity and quantum technology, although the findings should also be of interest to industry stakeholders who will be affected by new cryptographic standards.

The RAND Homeland Security Research Division

This research was conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division (HSRD). HSRD operates the Homeland Security Operational Analysis Center, a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Homeland Security. HSRD also conducts research and analysis for other federal, state, local, tribal, territorial, and public- and private-sector organizations that make up the homeland security enterprise, within and outside the Homeland Security Operational Analysis Center contract. In addition, HSRD conducts research and analysis on homeland security matters for U.S. allies and private foundations.

For more information on HSRD, see www.rand.org/hsrd. For more information on this publication, see www.rand.org/t/PEA2690-1.

Funding

Funding for this research was provided by gifts from RAND supporters and income from the operation of HSRD.

About the Authors

Alvin Moon is an associate mathematician at the RAND Corporation. His research papers have investigated theoretical models at the intersection of statistical mechanics and quantum information theory. He has a Ph.D. in mathematics.

Michael J. D. Vermeer is a physical scientist at the RAND Corporation. He is an expert on the cybersecurity risks created by quantum computing and the challenges with broad adoption of post-quantum cryptography. He has a Ph.D. in chemistry.