NIST Post Quantum Competition and Standardization

Syllab.io

SylLab Systems

NIST Post Quantum Competition and Standardization

Background

The asymmetric of public-key cryptographic algorithms in common use today rely on the fact that certain operations, such as multiplication and exponentiation, have polynomial complexity, while the operations required to undo them, factoring and discrete logarithms, have exponential complexity. This imbalance in complexity makes it possible to develop algorithms that are both usable and secure. However, with the advent of quantum computing, this will not always be the case, making new "post-quantum" algorithms necessary.

The National Institute of Standards and Technology (NIST) plays a critical role in developing standards for use in the United States that are often adopted internationally as well. Historically, NIST played a critical role in the standardization of the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) that it replaced. These algorithms do not rely on the "hard" problems that underly public-key cryptography, making them quantum-resistant. However, with the need for post-quantum algorithms, NIST has taken a leading role in the selection and standardization process.

The Need for Post-Quantum Cryptographic Algorithms

Classical asymmetric cryptographic algorithms based on the factoring and discrete logarithm problems have remained unbroken for several years. However, the advent of quantum computing poses a serious threat to the security of these algorithms.

The security of public-key cryptography depends on the asymmetric complexity of the underlying mathematical function. If a solution to the "hard" problem with polynomial complexity can be found, then the protocol falls apart. Even if cracking the cryptography requires several times more computational power than using it, a nation-state has the resources necessary to break any algorithm that could be run on a laptop or smartphone.

For the factoring and discrete logarithm problems, quantum computing poses an existential threat due to the existence of Shor's algorithm, which can solve the factoring problem in polynomial time. Once sufficiently large quantum computers become available, all classical asymmetric cryptography will be broken.

Quantum computing threatens the security of the underlying "hard" problems of classical asymmetric cryptography. However, other "hard" problems exist. Post-quantum cryptographic algorithms use other problems believed to be "hard" for quantum computers as well, including:

- Lattice
- Code-Based
- Hash-Based
- Multivariate
- Braid Group
- Supersingular Elliptic Curve Isogeny

Currently, no solutions with polynomial complexity exist for these problems, even with the advantages that quantum computers provide. As a result, these functions are the basis for the post-quantum cryptographic algorithms currently under development.

The NIST Post-Quantum Standardization Competition

NIST has a history of running competitions to identify the algorithms to be included in cryptographic standards. The DES and AES algorithms were selected based on an open submission process followed by multiple years of evaluating and comparing the various candidates. These multi-year competitions enabled the cryptography community to identify potential attacks against vulnerable algorithms and determine the relative efficiency and other performance characteristics of the various candidates for standardization.

In 2016, NIST kicked off a Post-Quantum Standardization Process designed to address the threat that quantum computers posed to asymmetric cryptography. A solicitation for post-quantum encryption algorithms and digital signature schemes resulted in 59 and 23 accepted submissions respectively.

Since the 2016 kickoff, NIST has hosted three PQC Standardization Conferences at which the current set of candidate algorithms was discussed. During these conferences, attendees could present attacks and other critiques of submitted algorithms, and the developers of the algorithms could provide updates. As part of this review process, multiple algorithms have been found to be vulnerable or withdrawn from the competition, and others have been weeded out based on various other factors.

The NIST competition is intended to have three rounds at the end of each only a subset of the candidates will move on to the next round. The finalists in Round 3 of the competition include four encryption algorithms and three digital signature algorithms as well as five encryption and three signature alternates. The results of Round 3 are anticipated to be announced in 2022, kicking off a process of developing standards for

the implementation and use of these algorithms. This standardization process is anticipated to last for several years with final standards being published in 2024 unless rapid advances in quantum computing force the process to be expedited.

Challenges of Implementing Post-Quantum Algorithms

NIST's Post-Quantum Standardization Competition is intended to lay the groundwork for a transition from classical to post-quantum algorithms. At the end of the process, standards will exist that define algorithms and configuration parameters for post-quantum cryptography.

However, while the competition solves the problem of selecting between many potential post-quantum candidates, it does not solve all of the challenges facing the adoption of post-quantum encryption. In its whitepaper, Getting Ready for Post-Quantum Cryptography, NIST outlines some of the challenges facing PQC, including the following.

Uncertain Quantum Computing Capabilities

The goal of post-quantum cryptography is to solve the problem that quantum computing poses to classical asymmetric cryptography. These algorithms are based on "hard" mathematical problems that are not "hard" for quantum computers. Once a quantum computer large enough to run Shor's algorithm becomes available, these classical algorithms are completely broken.

Post-quantum algorithms are designed to use mathematical functions that are believed to be "hard" for quantum computers as well as classical ones. However, the fact that the equivalent of Shor's algorithm for learning with errors (LWE) or other post-quantum "hard" problems doesn't exist now doesn't mean that it won't be discovered in the future. If this is the case, then any algorithms based on that "hard" problem will be broken as well.

Even if the "hardness" of the underlying mathematical functions of post-quantum candidates is not broken, these algorithms face other security risks. Compared to the algorithms in common use today, many of these algorithms are relatively new. Attacks against several vulnerable algorithms were discovered during NIST's multi-year competition, and finalists may be found to be vulnerable in the future.

Lack of Drop-In Post-Quantum Replacements

Asymmetric cryptography underpins most of the modern Internet. Encryption algorithms provide data privacy, digital signatures offer data integrity and authentication protections, and key exchange algorithms make it possible to develop shared secrets over a public channel.

The post-quantum cryptographic algorithms being standardized by NIST are intended to replace these insecure classical algorithms, providing protection against the effects of quantum computing. However, many of the candidates in NIST's competition have features that make them unsuitable as drop-in replacements for their classical counterparts. Examples include:

- Excessive digital signature sizes
- Large public and private keys
- Excessive processing requirements
- Operations that are asymmetric between senders and receivers

If post-quantum algorithms can't be slotted into existing protocols to replace existing, classical ones, then these protocols will need to be revised or replaced to accommodate them. This makes the transition to post-quantum cryptography much more complex, and, in some cases, these modifications may be infeasible. For example, legacy systems may not be capable of handling the large signature sizes or processing requirements of some candidate algorithms.

Widespread Usage of Cryptography

Cryptography provides multiple benefits, which has contributed to its widespread usage across IT systems. However, this same general adoption creates challenges when it becomes necessary to replace cryptographic algorithms.

The NIST PQC Standardization Process will specify how post-quantum algorithms should be used to replace classical ones. However, implementing these standards and replacing classical algorithms requires knowledge of where these algorithms are used within an organization's systems and software.

This poses a significant challenge for many organizations due to the widespread usage of cryptography. In addition to more visible applications of asymmetric cryptography, such as TLS, algorithms may be integrated into in-house software and legacy technology. Identifying and developing migration plans for these solutions using legacy encryption will be complex, and, in some cases, replacing classical algorithms with secure post-quantum ones may be infeasible or impossible, creating new security risks and challenges.

Next Steps for Post-Quantum Cryptography Deployment

The NIST PQC Standardization competition will select the post-quantum algorithms that will be included in standards. However, this is only the first step toward the widespread deployment of post-quantum cryptography.

Standards Development

NIST's competition for post-quantum algorithms is designed to identify the algorithms that will be included in standards for post-quantum cryptography. The process of developing the standards that define how these algorithms will be used will begin once the selected algorithms are announced.

While the announcement of the selected algorithms from Round 3 of NIST's competition is expected soon, the process of developing the standards will take several more years with an anticipated end date of 2024. Once these standards are developed, the process of implementing them and making the final transition over to post-quantum cryptography can begin.

Hybrid Algorithms

One of the biggest concerns about the post-quantum algorithms considered during NIST's contest is their relative youth and lack of in-depth security research. For example, several finalists are less than five years old, while commonly-used encryption algorithms, such as AES or RSA, have existed for decades.

To alleviate these concerns, the transition to post-quantum cryptography may include intermediate steps where classical and post-quantum algorithms are combined. Classical algorithms would contribute known resistance to non-quantum attacks, while post-quantum algorithms provide protection against future, quantum computing attacks.

Libraries and Standardized Implementations

The end result of the NIST process is standards defining how post-quantum cryptographic algorithms should be implemented. The actual implementation process can begin after those standards are complete.

Cryptographic algorithms standardized by NIST are commonly implemented across many different libraries. The creation of these standards-compliant libraries will help to speed the deployment of post-quantum algorithms because they make strong, quantum-resistant cryptography accessible to developers who are not experts in the field.

Migration Planning and Execution

One of the biggest challenges facing the deployment of post-quantum cryptography is the actual process of replacing quantum-vulnerable, classical algorithms with post-quantum ones. Cryptographic algorithms are used in various places, and identifying all instances of classical asymmetric cryptography within an organization may be difficult.

Once an organization has identified where vulnerable algorithms are in use, it can develop strategies for migrating to post-quantum replacements. In some cases, this

may involve updating to a new version of a standardized protocol; however, internal applications and legacy systems may require a more extensive migration process.

Preparing for a Post-Quantum Future

The NIST PQC competition and standardization process are designed to start the process of preparing organizations for the impacts that quantum computing will have on cryptographic security. Due to the complexity of the transition process and the significant impacts that quantum computers will have on data security, organizations should start the development and implementation of post-quantum migration plans as soon as possible.

SylLab Systems offers various solutions and support for organizations looking to integrate high-performance, efficient post-quantum cryptography into their applications, especially for resource-constrained IoT systems. For more information about how SylLabs can help with your organization's transition to post-quantum cryptography, schedule a meeting today or contact us at contact@syllab.io