What is Post-Quantum Cryptography?

Syllab.io

SylLab Systems

What is Post-Quantum Cryptography?

Introduction

The cryptographic algorithms in use today are secure against all known attacks using modern technology. While some attacks have been discovered that can reduce the security of commonly-used algorithms, no attack that can completely break the algorithms is currently feasible to execute.

However, this will not always be true. With the development of large quantum computers, which will be available within the near future, the security classical asymmetric or public-key cryptography will be broken.

The impeding threat to the security of classical cryptography has prompted the development of algorithms that are believed to be secure against both classical and quantum computers. These post-quantum cryptographic algorithms are an area of active development and will be rolled out to replace their quantum-vulnerable counterparts within the next few years.

Asymmetric Cryptography and "Hard" Mathematical Problems

Encryption algorithms are divided into symmetric and asymmetric cryptography. While symmetric cryptography uses the same secret key — and similar algorithms — for encryption and decryption, asymmetric cryptography uses a pair of related keys.

At the core of every asymmetric encryption algorithm is a mathematically "hard" problem. This means that performing a particular operation, such as multiplication, has polynomial complexity, while an operation that undoes it, such as factoring, has exponential complexity.

"Classical" public-key cryptography primarily uses one of two "hard" problems. These include the factoring problem — where multiplication is "easy" and factoring is "hard" — and the discrete logarithm problem — where exponentiation is "easy" and logarithms are "hard".

This asymmetric complexity is vital to the security of public-key cryptographic algorithms. Asymmetric encryption algorithms are designed so that a legitimate user, such as the sender and recipient of a message, only perform "easy" operations, while an attacker attempting to break the encryption would need to perform a "hard" operation.

The asymmetric complexity of the underlying "hard" problems of these cryptographic algorithms makes it possible to create encryption systems that are both usable and secure. Since the complexity of the "easy" and "hard" problems grow at different rates relative to the length of the secret keys used, a key length can be selected that makes legitimate use of the system — encryption and decryption — feasible while making it computationally infeasible for an attacker to crack the encryption.

The Quantum Computing Threat

The security of asymmetric cryptographic algorithms depends on the "hardness" of the underlying problem. The factoring and discrete logarithm problems work in these systems because the best-known methods of factoring the product of two prime numbers or calculating a logarithm have exponential complexity.

However, this is only true for classical — i.e. non-quantum computers. Quantum computers operate very differently from the computers in common use today. Bits in traditional computers can hold values of 0 or 1, but a quantum bit or "qubit" can be in a superposition of two states, simultaneously holding values of 0 and 1. This allows them to perform calculations in a different — and sometimes more efficient — way than a traditional computer, and quantum computing algorithms are designed to take full advantage of these differences.

One example of an algorithm designed specifically for quantum computers is Shor's algorithm. This algorithm is significant for "classical" asymmetric cryptography because it is capable of factoring the product of two prime numbers with polynomial — rather than exponential — complexity.

With a large enough quantum computer, Shor's algorithm breaks the asymmetry of the factoring and discrete logarithm problems. If both multiplication and factoring have polynomial complexity, then legitimate users have no built-in advantage over an attacker. Even if breaking encryption requires several times as much effort as encrypting a message, an attacker with sufficient resources can overcome that advantage.

Currently, quantum computers of the size needed to break modern public-key encryption are not available and will not be for several years. However, quantum computing and Shor's algorithm still pose a significant threat to data security today. Encrypted communications can be collected today and stored to be decrypted when the technology becomes available.

Developing Post-Quantum Algorithms

Mathematically "hard" problems are essential for asymmetric cryptography. They define the relationship between the public and private keys used for encryption and digital signatures, and they create the asymmetric relationship that makes the algorithms both usable and secure.

Quantum computing poses a threat to the "hard" problems used in classical public-key cryptography by providing "easy" solutions to them. However, these are not the only "hard" problems in existence.

Post-quantum cryptographic algorithms make use of other algorithms that are believed to be "hard" for quantum computers as well as classical ones. Examples of these include:

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

Algorithms based on these "hard" problems have been under development for several years now. However, this process has been accelerated by NIST's Post-Quantum Cryptography Standardization Process.

The NIST Post-Quantum Cryptography Standardization Process

The National Institute of Standards and Technology (NIST) has a strong history of running competitions to select algorithms for new cryptographic standards. The Data Encryption Standard (DES) of 1977 and the Advanced Encryption Standard (AES) of 2001 were both selected based on multi-year open competitions where publicly-submitted algorithms were discussed and analyzed by the community before NIST selected the winning algorithm.

In 2016, NIST launched a competition to select algorithms for new, post-quantum cryptographic standards. This included a call for proposals for both public-key encryption and digital signature schemes of which 59 and 23 algorithms were accepted respectively.

The NIST PQC Standardization process involves multiple rounds of review. During each round, attacks or other issues with an algorithm can be raised before the candidates moving on to the next round are selected and announced.

Currently, the competitions is in its third round with seven finalist and eight alternate algorithms. Once this round of competition is complete, standards will be created that define how these algorithms should be used to replace existing, insecure classical asymmetric algorithms.

Challenges of Post-Quantum Cryptography

NIST's PQC Standardization Process is designed to select the post-quantum algorithms that will be included in post-quantum standards. However, even after these algorithms are selected and announced, post-quantum cryptography still faces some significant. challenges.

Post-Quantum Algorithm Security

The goal of NIST's Post-Quantum Cryptography Standardization Process is to select the best available post-quantum cryptographic algorithms for standardization. These algorithms are selected via a multi-year process after receiving intense scrutiny from the cryptographic community.

However, these algorithms are intended to solve a problem that is not well defined or understood. Post-quantum cryptographic algorithms are designed to replace algorithms based on problems that are no longer "hard" for quantum computers. However, since these computers do not exist yet, determining what is "hard" or "easy" for them is difficult.

The existence of Shor's Algorithm proves that the factoring and discrete logarithm problems are insecure once large quantum computers are available. However, it is also possible that quantum algorithms will be developed that provide polynomial-time solutions to the "hard" problems used as the basis of modern post-quantum cryptographic algorithms.

Additionally, many of the algorithms included in NIST's contest are relatively new, especially when compared to the classical algorithms in common use today. During the competition, attacks were discovered that broke some candidate algorithms, and viable attacks on finalist algorithms may be identified in the future.

Lack of Drop-In Solutions

Asymmetric cryptographic is essential to the function of the modern Internet. Since the Internet grew up with classical asymmetric cryptography, the protocols in common use today are designed with them in mind.

Ideally, post-quantum cryptographic algorithms would be drop in replacements for their classical counterparts. However, the candidate algorithms under

consideration in the NIST contest have various issues that make this impossible, including:

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

The inability to simply drop in post-quantum replacements for classical algorithms complicates the process of addressing the threat that quantum computing poses to cryptography. Protocols using insecure algorithms will need to be revised or replaced, which may not be possible in some cases.

Visibility Into Cryptography Usage

Cryptography is the foundation for much of modern IT. It enables private and secure communications and ensures the integrity and authenticity of data.

Asymmetric cryptography's unique design means that it is more versatile than symmetric algorithm, and its many applications means that it is used in various ways. However, this creates significant challenges when the threat of quantum computing forces an update to new, post-quantum algorithms. Organizations will have to identify where classical asymmetric cryptography is used within their environments — including in legacy systems — and develop strategies for updating them.

Deploying Post-Quantum Cryptography

NIST's PQC Standardization Competition is designed to identify the post-quantum cryptographic algorithms that will replace the quantum-vulnerable, classical algorithms in common use today. However, this is only the first stage in the process of deploying post-quantum cryptographic algorithms.

Once the results of NIST's competition are announced, some of the next steps toward the widespread deployment of post-quantum cryptography include:

- **Standards Development**: The result of the NIST PQC competition will be a list of the algorithms to be included in post-quantum cryptographic standards, not the standards themselves. Once the finalists have been selected and announced, the process of developing the standards will take several more years with an anticipated completion date in 2024.
- **Hybrid Solutions**: The relative youth of many post-quantum cryptographic algorithms is a common concern as a lack of cryptanalytic research could mean that finalist algorithms may contain undetected vulnerabilities.

Hybrid protocols combining classical algorithms' resistance to non-quantum attacks with post-quantum algorithms may be a transitional step on the path to the full deployment of PQC.

- **Standardized Implementations**: Once standards have been developed for post-quantum cryptographic algorithms, the next step is the development of libraries and implementations of these algorithms that follow the standards. These implementations lay the groundwork for integration of standardized PQC algorithms into applications and protocols.
- **Post-Quantum Migration**: With standards and implementations in place, mass migration to post-quantum algorithms can occur. This includes both updates to widely-used protocols such as TLS and organizations individually identifying and updating classical asymmetric cryptography within their environments to use post-quantum algorithms.

Preparing for a Post-Quantum Future

Large-scale quantum computing poses a significant threat to the security of the cryptographic algorithms in common use today. Once sufficiently large quantum computers are available, Shor's algorithm will break classical asymmetric cryptographic algorithms based on the factoring and discrete logarithm problems.

While quantum computers are still several years in the future, "store now, decrypt later" attacks pose a significant threat to data security today. An attacker that collects data encrypted with quantum-vulnerable algorithms today can decrypt them and access potentially sensitive information when the technology becomes available. Making the transition to post-quantum cryptography as soon as possible is essential to corporate data security.

SylLab Systems offers various solutions and support options designed to ease companies' transitions to high-performance post-quantum cryptographic algorithms. To learn more about starting your post-quantum transition, schedule a meeting today or contact us at contact@syllab.io.