ITL BULLETIN FOR FEBRUARY 2018

SECURING TOMORROW'S INFORMATION THROUGH POST-QUANTUM CRYPTOGRAPHY

Dustin Moody, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms.

In particular, quantum computers would completely break many public key cryptosystems, including Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and elliptic curve cryptosystems. These cryptosystems are used to implement digital signatures and key establishment. They play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks. Table 1 summarizes the impact of large-scale quantum computers on common cryptographic algorithms, such as RSA and the Advanced Encryption Standard (AES). It is not known how far these quantum advantages can be pushed, nor how wide is the gap between feasibility in the classical and quantum models.[2]

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sized needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

[2] NISTIR 8105*, Report on Post-Quantum Cryptography*, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

The question of when a large-scale quantum computer will be built is complicated and contentious. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some experts predict that within the next 20 or so years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing-resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

Due to this concern, many researchers have begun to investigate *post-quantum* cryptography (PQC) (also called *quantum-resistant* or *quantum-safe* cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers. These algorithms could serve as replacements for our current public key cryptosystems to prepare for the eventuality that large-scale quantum computers become a reality.

Quantum-Resistant Cryptography and NIST Approach

At present, there are several post-quantum cryptosystems that have been proposed, including lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, hash-based signatures, and others. Research continues as the industry gains more confidence in the security of these systems - particularly against future adversaries with quantum computers - and to improve cryptosystems' performance.

NIST has determined that this is a prudent time to begin developing standards for post-quantum cryptography. One factor driving this timing is the recognition there has been noticeable progress in the development of quantum computers. Researchers are making headway in the development of theoretical techniques for quantum error correction, fault-tolerant quantum computation, and experimental demonstrations of physical qubits and entangling operations in architectures that have the potential to scale up to larger systems.

A transition to post-quantum cryptography is very unlikely to be just a simple "drop-in" replacement for current public-key cryptographic algorithms. Developing, standardizing, and deploying new post-quantum cryptosystems will require significant time and effort. Such a transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs. Therefore, it is desirable to plan for this transition early.

NIST has started the process to develop new cryptography standards. The team began by soliciting public comments on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. A public call for nominations for post-quantum candidate algorithms was completed in late 2017, and Round 1 Submissions are available for review and comments from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions. NIST is now in the evaluation phase and expects to perform multiple rounds of evaluation over a period of three to five years. The goal of this process is to select a small number of candidate cryptosystems for standardization.

NIST anticipates that the evaluation process for these post-quantum cryptosystems may be significantly more complex than the evaluation of the SHA-3 and AES candidates in consideration of the following factors:

- The requirements for public-key encryption and digital signatures are more complicated;
- The current scientific understanding of the power of quantum computers is far from comprehensive; and,
- Some of the candidate post-quantum cryptosystems may have completely different design attributes and mathematical foundations, so that a direct comparison of candidates would be difficult or impossible.

Because of these complexities, NIST believes that the post-quantum standards development process should not be treated as a competition; in some cases, it may not be possible to make a well-supported judgment that one candidate is "better" than another. Rather, NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public, and the team will encourage the cryptographic community to also conduct analyses and evaluation. This combined analysis will inform NIST's decision on the subsequent development of post-quantum standards.

The resulting new standards will be used as quantum-resistant counterparts to existing standards, including digital signature schemes specified in Federal Information Processing Standards (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SPs) 800-56 A and B. The process is referred to as *post-quantum cryptography standardization*. The standards will be published as Federal Information Processing Standards or Special Publications.

Evaluation Process

NIST has formed an internal selection panel of NIST employees for the technical evaluations of the submitted algorithms. This panel will analyze the submitted algorithms for security suitability and performance characteristics. The panel will review public comments received in response to the posting of the "complete and proper" submissions. The panel's review will consider all presentations, discussions, and technical papers presented at the PQC standardization conferences, as well as other pertinent papers and presentations made at other cryptographic research conferences and workshops. NIST will issue a report after each PQC standardization conference. Final selections of cryptosystems will be made by NIST, and the technical rationale for these decisions will be documented in a final report.

Conclusion

The next important step will be the first PQC Standardization Conference, co-located with the Ninth International Conference on Post-Quantum Cryptography (PQCrypto) in April 2018. The aim of the PQC Standardization Conference is for submitters to present their algorithms and design rationale, and for researchers and practitioners to ask questions on the submitted algorithms.

During the next three-to-five years, NIST will perform analysis, report findings, and conduct several workshops, after which NIST will produce draft standards.

Additional Resources

NIST's Post-Quantum Cryptography page – https://csrc.nist.gov/projects/post-quantum-cryptography

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov