Mitigating the Quantum Threat with Hybrid Cryptography

cloud security alliance®

ACKNOWLEDGEMENTS

Main Author:

Roberta Faux

Co-chairs:

Bruno Huttner

Ludovic Perret

Reviewers:

Jon Lau

CSA Staff:

Hillary Baron

TABLE OF CONTENTS

QUANTUM THREAT BACKGROUND

The dawn of quantum computing threatens the global cryptographic infrastructure. Large-scale, cryptographically relevant quantum computing will render today's classical public key algorithms insecure. This paper will not address the effects of diminished security on symmetric algorithms. There are cryptographically hard problems believed to be secure against even quantum attacks, and the cryptosystems based on these problems are interchangeably called quantum-safe, quantum-proof, post-quantum or quantum-resistant[1]. This quantum-safe cryptography has received increasing attention in academic communities, as well as from industrial players.

In this paper, the following terms will be referenced:

- "Classical Key Exchange" refers to a public-key cryptographic algorithm in use today. Such algorithms include Rivest-Shamir-Adleman (RSA), Diffie-Hellman, and Elliptic Curve Diffie-Hellman (ECDH). These schemes are secure against attacks using classical computers but are not secure against attacks using a sufficiently large quantum computer.
- "Quantum-Safe Key Exchange" is a key exchange algorithm that is secure against an attack by both classical computers and quantum computers.
- "Classical Digital Signature" refers to digital signatures generated by algorithms used today that are secure against attacks from classical computers, but not from sufficiently large quantum computers. Such algorithms include RSA, the National Institute of Standards and Technology Digital Signature Algorithm (NIST DSA), the NIST Elliptic Curve DSA (ECDSA) and the Edwards Elliptic Curve DSA (EdDSA).
- "Quantum-Safe Digital Signature" is a digital signature algorithm that is secure against an attack by both classical computers and quantum computers.

The worldwide pace of quantum research and development is staggering, with significant investments being made by approximately 50 companies. Regardless, opinions vary widely concerning timelines on when quantum computers will develop the capacity to solve problems that classical computers practically cannot.

In reality, there already exists very small quantum computers, but practical scaling challenges pose a major obstacle to further innovation. There are different approaches available to address this issue, including the implementation of superconductors, topology, and ion traps; however, each of these approaches has theoretical and engineering hurdles.

Furthermore, myriad variables make it difficult to predict—with any degree of precision—when a large-scale quantum computer will threaten today's security structure. According to mathematician Dr. Michele Mosca, there is "a 1/7 chance of breaking RSA-2048 by 2026 and 1/2 chance by 2031."[2] Yet skeptics, such as Yale professor and mathematician Gil Kalai raise doubts that quantum computers will every be viable.[3]

---

[1] For an explanation of the technical terms used throughout the paper, we refer to the Glossary published by the QSS: https://cloudsecurityalliance.org/artifacts/quantum-safe-security-glossary/

[2] Michele Mosca, Cybersecurity in an era with quantum computers: will we be ready? https://eprint.iacr.org/2015/1075.pdf 2015.

[3] https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/

Typically, cybersecurity experts tend to predict security threats will be realized sooner than do quantum computing companies.

Regardless of predictions, society has a vested interest in monitoring and regulating quantum computer development and the threats it may pose to cybersecurity infrastructure. All stakeholders agree that whenever cryptographically relevant quantum computers are finally realized, classic key exchanges and classic digital signatures will be rendered vulnerable. There is enough concern that standards bodies worldwide are actively engaging in efforts to standardize quantum-safe solutions in the near term.

STANDARDS ORGANIZATIONS

International standards bodies in Europe, the United States, and other regions are moving forward with quantum-resistant cryptography. In 2015, the European Telecommunications Standards Institute (ETSI) published a white paper urging stakeholders to begin action for investigating and adopting quantum-safe cryptography. In August 2015, the U.S. National Security Agency (NSA) released a notice to revamp Suite B Cryptography to include quantum-safe cryptography. Additionally, NIST concluded a call for proposed quantum-safe algorithms in November 2017, and currently plans to implement standards by 2025. As the NIST process moves forward, other standards organizations—such as the International Telecommunication Union (ITU) and the Internet Engineering Task Force (IETF)—are actively working to incorporate quantum resistant standards.

INTRODUCING HYBRID SCHEMES

What is a Hybrid?

Hybrid schemes provide both the classical security of classical crypto and the quantum security of a quantum-safe system.

In the context of this discussion, a hybrid cryptosystem is one which combines two or more different cryptographic techniques to perform the same function. The security of a hybrid scheme will remain as long as at least one of its two underlying cryptographic schemes remains secure—a so-called "belt and suspenders" approach. Until the quantum computer threat, cryptographers had sufficient confidence in the widely used classical public-key systems and did not rely on hybrid schemes.

For this reason, one does not typically see, for example, both RSA and ECDH being used to secure a single communications link. However, many of the quantum-safe cryptosystems are much newer than classical systems, and they have not been subjected to the same level of scrutiny and analysis as the classic systems. Therefore, there exists apprehension in the crypto community that further research could significantly reduce the classical security of some of these quantum-safe systems.

Cost of Hybrids

Hybrids—while likely necessary in some instances—are costly in many ways: they are slower, they introduce a larger footprint for key storage, and are less efficient. Without any standards in place for

hybrids or quantum-safe cryptography, there is an increased risk of implementation flaws—which may pose a more significant threat than even a large-scale quantum computer. A faulty implementation may lead to a less-secure hybrid cryptographic system infrastructure. Classical quantum-safe hybrids may be appropriate given the novelty of many quantum-safe schemes and the lack of standards (and are likely necessary for the near term as a transitory solution). However, in the long run, hybrid schemes may become too burdensome.

Who Might Need a Hybrid?

There are two types of organizations that need to consider quantum-safe solutions today (i.e., before the adoption of standards). One group includes organizations tasked with protecting data over an extended duration, such as government entities, law firms, financial service providers, medical researchers, and pharmaceutical companies. Internal human resource teams and organizational departments with ties to legal and Internet Protocol-specific data would also fall into this category. These organizations should be concerned with adversaries (or competitors) who could intercept, collect and store sensitive data today for decryption at a later time, when a sufficiently large quantum computer is available.

The second group includes organizations that use embedded systems for cryptography, but also have a limited capacity to modify their infrastructure. For instance, some microprocessors have a three- to 10-year development cycle, and often a 10- to 20-plus-year lifecycle. Typically, embedded systems should last decades. Sectors employing such infrastructure include those working in aerospace, finance, military, automotive connectivity, medical electronics and imaging, data processing, and telecom.

Organizations designated to one of these two categories are at the highest risk and must consider migrating to quantum-safe cryptography soon. Other sectors can likely wait until standards are in place.

Organizational decisions must be made probabilistically regarding quantum-safe solutions, especially considering the hazy timeline and numerous "unknowns" associated with quantum computing development. Considerations should include a clear and accurate evaluation of possible risks, and answer—at a minimum—the following questions, as stated previously.

- How long does the organization's information need to be protected?
- How long will it take to upgrade the organization's infrastructure?

Organizations must consider the hybrid approach if they calculate that their current housed data—secured through classical crypto infrastructure—will still need protection once the quantum safe computer is developed. Without the transition to a hybrid model now, data will likely be vulnerable to compromise later.

HYBRID OPTIONS

There are several options for hybrids. This paper will cover four: (1) classical/quantum-safe; (2) quantum-safe/quantum-safe; (3) classical/ quantum key distribution (QKD) and; (4) classic asymmetric/symmetric

Classical/Quantum-Safe Hybrids

Organizations that need immediate quantum-safe security implementation can now migrate to a classical/quantum-safe hybrid system. For U.S.-dominated sectors, meeting the guidelines established in the Federal Information Processing Standard (FIPS) 140-2 is often a requirement for this transition. Currently, FIPS 140-2 only validates the NIST-approved (classical) components, but it does allow for non-FIPS layers to be introduced[4]. Hence, a hybrid scheme that uses both a classical and a quantum-safe algorithm can be implemented.

Systems are at least as secure against a classical attack as the classical public-key system alone, and there is also some degree of security against a quantum attack utilizing this hybrid model.

A classical/quantum-safe hybrid provides an effective way to test the performance of quantum-safe cryptography in a real-life setting without putting the present-day security of network users at-risk. There have been several notable classical/quantum-safe hybrid experiments, and they have been instrumental in demonstrating that the real-life performance of quantum-safe cryptography is acceptable. For instance, Google experimented with a hybrid mode using an elliptic curve classically secure cryptosystem with a quantum-resistant lattice scheme[5].

Quantum-Safe/Quantum-Safe Hybrids

Currently, organizations that do not need to meet the FIPS 140-2 compliance requirements are allowed to migrate if they have enough confidence in their proposed quantum-safe algorithm selections.

For data needing protection today as well as quantum security in the future, consider creating a hybrid of two quantum-safe cryptosystems. This model—as opposed to a classical/quantum-safe hybrid system (where the classical part of the hybrid will become insecure with the advent of a quantum computer)—may provide desired versatility. Security of the overall hybrid scheme will remain strong as long as either of the quantum-safe algorithms remains secure. A reasonable way to choose the two quantum-safe algorithms for a hybrid would be to use algorithms based on two different, hard mathematical problems. For example, this combination might include supersingular isogeny key encapsulation (SIKE)—based on supersingular isogenies of elliptic curves—coupled with a problem rooted in the mathematics of lattices. By combining these two algorithms into a hybrid scheme, the security of the hybrid remains intact as long as one of these algorithms remains unbroken.

For high-confidence, quantum-safe protection—particularly in light of the uncertainty regarding the security of quantum-safe cryptographic algorithms—it is advisable to create a hybrid from two quantum-safe algorithms rather than from a classical and a quantum-safe algorithm.

Classical/QKD Hybrids

Quantum key distribution (QKD) systems can be combined with other cryptographic tools to create hybrid classical/QKD systems. Indeed, all commercial applications of QKD recommend such an

[4] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8019.pdf

[5] https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

approach, mixing—for example—classical key exchange with QKD in link encryptors. Unlike cryptographic algorithms that rely on the assumption of the computational difficulty of specific mathematical functions, QKD derives its security from the foundations of quantum mechanics. Adopting a classical/QKD hybrid, when practical, reduces the uncertainty remaining with the other hybrid methods. Another way to create a simple classical/quantum-safe hybrid is to utilize existing classical key exchanges—such as Transport Layer Security (TLS) or Internet Key Exchange (IKE)—at the application or network layers of a protocol stack while using symmetric key cryptosystem keyed with a QKD system at the link layer of the protocol stack. The use of different cryptographic principles at different layers of the protocol stack enhances the security of the complete system.

Classical Asymmetric/Symmetric Hybrids

The three previous hybrid schemes describe methods for mixing two key establishment schemes. Another approach: have a secret that is shared out-of-band before establishing a connection. This technique is best suited to closed environments where connections can be configured manually, and the key management overhead isn't prohibitive. In this scheme, the classical asymmetric portion provides for the protocol to maintain existing perfect forward secrecy guarantees while mixing in a 256-bit symmetric key to provide quantum resistance. This scheme offers long-term confidentiality when QKD is not available or practical.

During the transition period to quantum-safe schemes, this hybrid approach is able to combine a quantum-safe asymmetric scheme with pre-shared symmetric keys. This provides protection in the event the quantum-safe scheme suffers a cryptographic break.

HYBRID CAUTION

Cryptographic implementation can be challenging, and the threat of a flawed execution might be more dangerous than a quantum computer. Often, security breaches do not come from brute force attacks but from the exploitation of implementation mistakes. A minor error in configuration or coding may inadvertently remove a significant degree of protection—or even render the crypto implementation useless against attacks. There is a real need to standardize the hybrid key exchange format and ensure a formal security analysis considering these hazards. It is questionable how much security a hybrid model may provide—if any—without careful thought.

CONCLUSION

For some organizations, where long-term data protection is essential or where new systems are designed to remain in operation for an extended period, hybrids offer a degree of security from the threat of quantum computing. However, the choice of which hybrid system to implement will depend on results gleaned from organizational threat modeling. For organizations that are not concerned about "harvest now, decrypt later" threats, it may be prudent to wait for the development of universal standards before deploying a hybrid defense. This delay may also help avoid the possibility of implementation flaws.

