The State of Post-Quantum Cryptography

Presented by the Quantum Safe Security Working Group

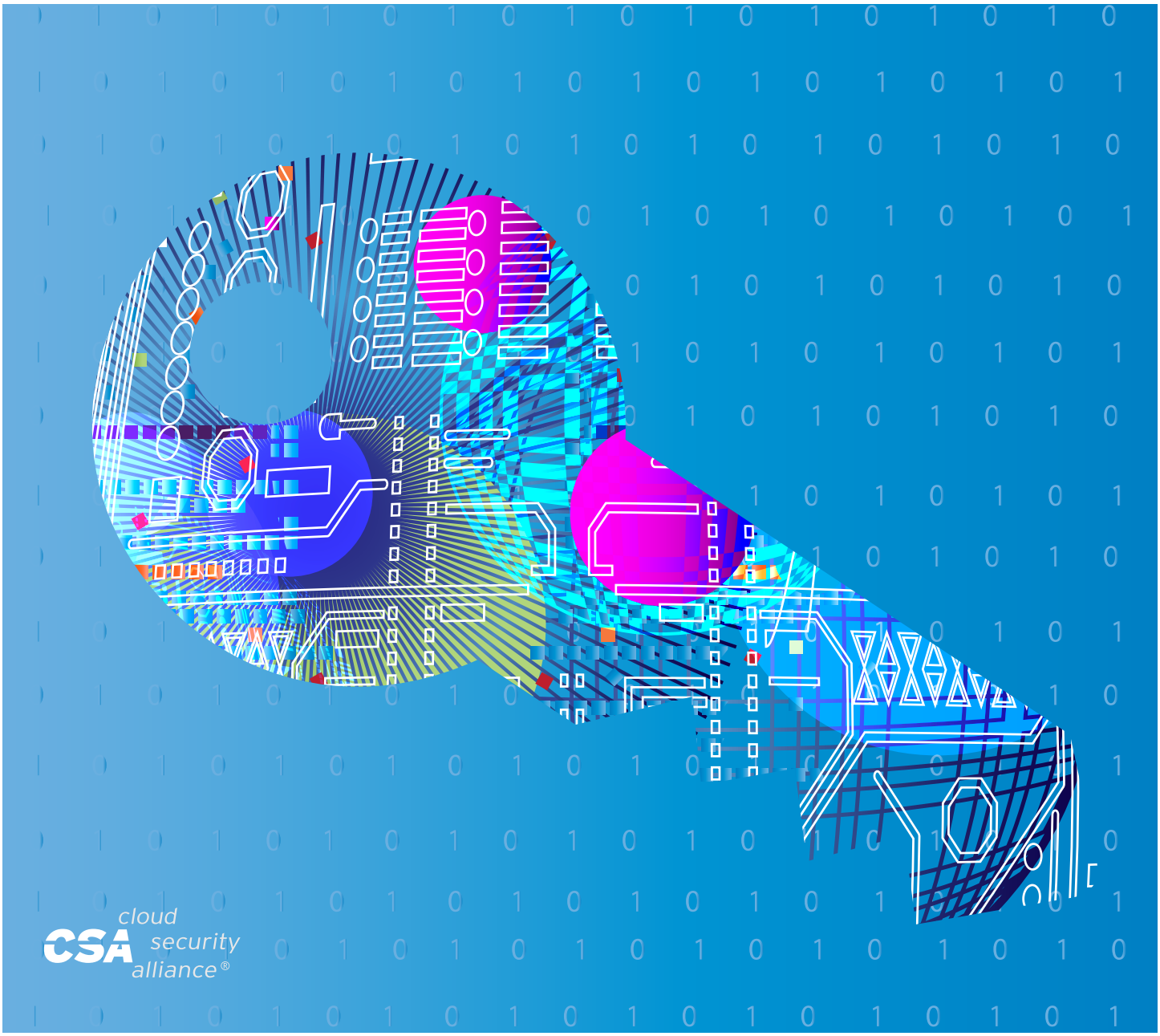

TABLE OF CONTENTS

ABOUT CSA

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at www.cloudsecurityalliance.org and follow us on Twitter @cloudsa.

ACKNOWLEDGMENTS

Lead Author:

Roberta Faux

Quantum Safe Security Working Group Co-Chairs:

Bruno Huttner
Jane Melia

Cloud Security Alliance:

Hillary Baron
Ryan Bergsma
Kendall Scoboria

WHAT IS POST-QUANTUM CRYPTOGRAPHY?

Most people pay little attention to the lock icon on their browser's address bar that signifies a secure connection called HTTPS. This connection establishes secure communications by providing authentication of the website and web server as well as encryption of communications between the client and server. This happens each time a person uses PayPal, sends a Gmail message, or logs into Facebook. If the connection is not secure, then a user may be vulnerable to malicious exploits such as malware injection, hijacking of financial transactions or stealing the user's private information. The encryption behind HTTPS is the cornerstone of online security and privacy, and the lack of secure internet communications could devastate modern life in the digital age, rendering the internet vulnerable in nearly every aspect imaginable.

This scenario is a growing concern in the next decade as the reality of quantum computers draws near. Quantum computers will have the technology to break the current public key infrastructure which is the backbone of internet security.

Researchers worldwide are working to make quantum computing a reality. Microsoft, Google, IBM, Intel, and many governments are working on building the first large-scale quantum computer. Today, RSA, Diffie—Hellman (DH) and Elliptic Curve-based are ubiquitously used for the global public key infrastructure. All of these algorithms are vulnerable to quantum attacks. Fortunately, there are alternative classes of public key algorithms developed which are believed to be resistant to quantum computing attacks.These algorithms are called post-quantum, quantum-safe, or quantum-resistant algorithms. A transition to these algorithms will provide continued protection of information for many decades to come.

In light of the threat of quantum computing and the emergence of post-quantum cryptography, both European and U.S. standards bodies are exploring quantum resistant (QR) cryptography. In 2015, the European Telecommunications Standards Institute (ETSI) published a white paper urging stakeholders to begin investigating and ultimately adopting QR cryptography. In August 2015, the U.S. National Security Agency posted a notice that reinforced the need for U.S. national security systems to begin planning for the replacement of current public key cryptography with quantum-resistant cryptography. In November 2017, the National Institute of Standards and Technology (NIST) concluded its call for submission of quantum-resistant cryptographic algorithms and initiated the process for review and standardization in the 2022-2025 time period.

Cryptographic transitions take time, often a very long time. For instance, the call for increased RSA key size from 1024- to 2048-bit, or the call for the transition from RSA to elliptic curve-based cryptography took over a decade. The transition to quantum-resistant cryptography is likely to take at least ten years. Some quantum computing experts believe that quantum computers with the ability to break RSA and Elliptic Curve Cryptography (ECC) may be available within ten to fifteen years. It is therefore important to plan for transition as soon as possible.

BREAKING PUBLIC KEY CRYPTOGRAPHY

Current secure HTTPS communications rely on the use of public key cryptography to securely establish a cryptographic key between two parties. Public key cryptography is used not only to protect the secrecy of the keys established between the parties but is also used to bind identity information to the keys in such a way that each party has an assurance of the identity of the other party. Once these keys are exchanged, the data is then encrypted with symmetric cryptography, such as the U.S. Advanced Encryption Standard (AES).

In 1994, a mathematician named Peter Shor developed an integer factorization algorithm that runs on a quantum

computer. Large-scale quantum computers will be able to use Shor's algorithm to break all public key systems that employ RSA (integer factorization-based), Diffie—Hellman (finite field discrete log-based), and Elliptic Curve (elliptic curve discrete log-based) Cryptography. These algorithms underpin essentially all of the key exchange and digital signature systems in use today. Once reasonably sized quantum computers capable of operating on tens of thousands of logic quantum bits (qubits) exist, these public key algorithms will become useless.

Symmetric key cryptographic algorithms like the AES are much less susceptible to attack by a quantum computer. A quantum algorithm known as Grover's algorithm can reduce the cost of attacking a symmetric cryptographic algorithm. If a cryptographic algorithm has a key size of n bits, Grover's algorithm can theoretically reduce the security of that algorithm to one with a key size of n/2 bits. However, by simply making key sizes larger, the same symmetric cryptographic algorithms with confidence. If one is using AES with 128-bit keys today, one should consider moving to AES with 256-bit keys by the time large-scale quantum computers exist. For hash algorithms, Grover's algorithm provides non-trivial speedup on a quantum computer. Currently, it is recommended that the sizes of hash should be increased by a factor of two to compensate for the speedup. Generally, 256-bit hashes are considered safe against quantum computing attacks.

KEY EXCHANGE AND DIGITAL SIGNATURES

There are two processes that use public key cryptography: key establishment and digital signatures. Within key establishment, there are two common methods: key agreement and key transport.

Key transport uses a public key encryption system. Party A generates a key. Party A then gets the public key for Party B, encrypts the key it had generated, and sends the resulting cipher to Party B. Party B uses its private key to decrypt the cipher and recover the key that A generated. Parties A and B then use that key in a symmetric cryptographic algorithm.

In a key agreement, parties A and B generate new public keys and corresponding private keys and exchange the public keys. Given the exchanged information, each party then uses its private key to create a shared secret key that acts as the key in a symmetric cryptographic algorithm.

Public key cryptography is also used for digital signatures. Through the use of digital signatures, the recipient of a message can gain some assurance that the message came from the party holding the private key used to sign the message. The public signing key is normally bound to a party's identity by having a commonly trusted party digitally sign the concatenation of a party's identity and their public key. This is the foundation of a Public Key Infrastructure (PKI), whereby a trusted party provides its public key to all other parties in a network. The trusted party uses its corresponding private key to sign the concatenation of every other party's identity and their public key. The concatenation of the identity of a party, its public key, and the trusted party's signature is called a "certificate." When Party A wants to send a signed message to Party B, it uses its private key to sign the message creating a signature. Party A then sends the message, its signature and its certificate to Party B. Party B verifies the trusted party's signature on the certificate, extracts A's public key, knowing now that Party A holds the corresponding private key and then verifies the signature on the message.

There are two significant risks in delaying a move to quantum-resistant cryptography. First, when considering information that needs to be kept confidential for many decades, there is the danger that an attacker could store off ciphertext and key establishment data that isn't protected with quantum resistant cryptography today and then break it with a quantum computer in the future. Information with a significant value well into the future should be protected against quantum computing attacks as soon as feasible.

Second, there is a risk that digitally signed data may not be trustworthy in the future. If one is using a system that digitally

signs data today with a non-quantum resistant digital signature, an attacker with a quantum computer in the future could change the signature or repudiate ever signing some information. The chain of trust would be broken. Once quantum computers are able to break signatures, the threats are widespread. For example, a hacker could break a Windows software update key and send fake updates (malware) to a computer. Hence, the need to implement quantum-resistant cryptography is not relegated to sometime in the future, but is of real import today.

THE ALTERNATIVES

There are currently many choices for quantum-resistant cryptography. Some standards organizations have begun a process of reviewing candidate algorithms to create standards out of a set of those algorithms that pass public review. Quantum-resistant cryptographic algorithms are based on a variety of different mathematical principles. The major categories of algorithms are explored below:

Lattice-Based Cryptography

Lattice-based cryptography is very attractive for post-quantum solutions. Some of these algorithms have strong security reductions to fundamentally difficult mathematical problems. Lattice-based cryptography generally offers very fast implementations. Provably secure reductions exist for lattice-based key agreements based on:

1. Learning with Errors (Microsoft's FRODO scheme is an example)
2. Ring Learning with Errors (the New Hope scheme is a popular example)
3. Module Learning with Errors (the Kyber scheme is a leading example)

The NTRU Encrypt system is a public key encryption scheme that can be used for key transport. Although it does not have a strong security reduction, it has been studied for many years and exists in IETF and ANSI standards. Both FRODO and New Hope can be used for public key encryption as well.

There are also several lattice-based signature algorithms. Leading examples include:

1. Learning with Errors (a scheme called TESLA or a scheme by Bai and Galbraith are examples)
2. Ring Learning with Errors (the GLP signature based on the work of Gunesyu, Lyubashevsky, and Poppelmann is an example)
3. Module Learning with Errors (the DILITHIUM scheme is the leading example)

There is also the patented NTRUSign scheme and BLISS, which use trapdoor lattices to create effective signature schemes.

With all of these schemes, it is important to note that parameter selection is complex. Bigger key sizes are not always more secure key sizes and care must be taken in selecting parameters that balance efficiency and security in an effective way.

Hash-Based Schemes

Hash-based schemes are a promising alternative for signatures. Hash-based schemes include cryptographic systems such as Lamport signatures and Merkel signatures. They have received significant academic study over several decades of research. Two hash-based signature systems, LMS & XMSS, have been proposed in standards organizations. The hash-based signatures known as LMS and XMSS are widely accepted as secure when used with a strong hash function. There have also been recent advances in hash-based signatures such as SPHINCS which does not require a signer to remember a history of its past signatures in order to be secure. These schemes offer the benefit of having a small public key size with

efficient signing and verification algorithms. However, the signatures they produce are large and there is a limit on the number of messages that can be securely signed using a given private key.

Elliptic Curve Isogenies

Although standard Elliptic Curve Cryptography (ECC) is easily broken with a quantum computer, one can use other properties of elliptic curves to create a quantum-resistant key agreement scheme like Diffie—Hellman (DH) or Elliptic-curve Diffie—Hellman (ECDH). A quantum-resistant key exchange can be built from the isogenies (mappings between different elliptic curves) of Supersingular Elliptic Curves. This quantum-resistant algorithm was first published in 2011 and has undergone significant scrutiny in the years since. An important feature of this scheme is that the required key size is similar to the currently supported (non-Elliptic) Diffie—Hellman key exchange. This algorithm is popularly known as SIDH (Supersingular Isogeny Elliptic Curve Diffie—Hellman) or SIKE (Supersingular Isogeny Key Exchange). Also, this algorithm can use some of the same computational elliptic curve primitives used in normal Elliptic Curve Cryptography. This makes SIDH a relatively straightforward upgrade to systems already using ECC. While there are several complex isogeny calculations, the overall flow of the method is easy to understand for someone familiar with Diffie—Hellman cryptography and elliptic curve mathematics.

Multivariate Cryptography

Multivariate cryptography is based on the difficulty of solving systems of multivariate polynomials over a finite field. Solving these systems of multivariate equations is considered a fundamentally hard problem, even for a quantum computer, and thus a good basis for quantum resistant cryptography. There a number of signature algorithms, including Unbalanced Oil and Vinegar and Rainbow. There are multivariate schemes for both symmetric and asymmetric cryptography that can offer some advantage in a constrained environment. These algorithms offer very fast arithmetic over small binary fields so the computational overhead for key encryption or signature is low, however public key sizes are very large.

Code-Based Cryptography

Cryptography-based one-error correcting codes, or code-based cryptography, is another class of quantum-resistant systems with no known quantum attacks. Specific algorithms include the long-studied McEliece and Niederreiter systems that date back more than 30 years. There are also newer code-based algorithms, like the Code-Based Algorithm for Key Encapsulation (CAKE) system, published in 2017. While the public key for the McEliece and Niederreiter schemes is huge and a significant obstacle to their practical utility, the CAKE scheme employs a number of tricks that overcome this obstacle and make it relatively useful.

CHALLENGES

While quantum-resistant cryptography can perform the same functions as the existing generation of public key cryptography (which can be exploited by a quantum computer), there are some important challenges. Most post-quantum algorithms require significantly larger key sizes than existing public key algorithms. This results in remarkably larger amounts of data that need to be sent over a communications link for key establishment and signatures. These larger key sizes also require more storage inside a device. However, while key sizes are larger, most quantum-resistant algorithms are more computationally efficient than existing public key algorithms.

In order to gain quantum-resistant protection for information before standards bodies like NIST and ETSI have completed their cryptographic evaluations of the various algorithms, some experts are suggesting the use of hybrid key agreement schemes that combine the results from two different key exchanges to create a single key. For instance, Google

experimented with using a hybrid of an Elliptic Curve key agreement along with a Ring Learning with Errors key agreement into the Google Chrome Canary browser. In the Internet Engineering Task Force's Transport Layer Security Working Group, there is a proposal for a "Quantum Safe Hybrid" ciphersuite. Most of the proposed hybrids involve a classical public key system with a quantum-resistant public key system. However, there is the possibility that a quantum computer will be in an adversary's hands in ten to fifteen years, so it may be better to consider a hybrid of two quantum resistant algorithms (like SIDH and Ring Learning with Errors). Both of these have a good chance of remaining robust even when a quantum computer exists. In a classical/quantum-resistant hybrid, the user will be left with just the single quantum-resistant algorithm when quantum computers do exist.

POST-QUANTUM CRYPTOGRAPHY VS. QUANTUM CRYPTOGRAPHY

Post-quantum cryptography is different from quantum cryptography, which is the use of quantum technology for communication and computation to protect messages. The best-known example of quantum cryptography is Quantum Key Distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties without a third party learning anything about that key. This is achieved by encoding the bits of the key as quantum data, which will be disturbed if observed by a third party. The key is then used with conventional symmetric encryption or authentication techniques. QKD has been explained in a previous white paper published by the Cloud Security Alliance's Quantum-Safe Security Working Group and can be downloaded here. It is likely that both QKD and post-quantum algorithms will find their applications in the future post-quantum cryptographic world.

CONCLUSION

Practical quantum computing is growing closer to becoming a reality. This technology will bring massive disruption to a wide range of industries, from space exploration to intelligence gathering, artificial intelligence to medical research. Simultaneously, it places us on the horizon of a grave threat to the security of global communications posed by quantum computing. It is key to begin planning now for a future with quantum computing.