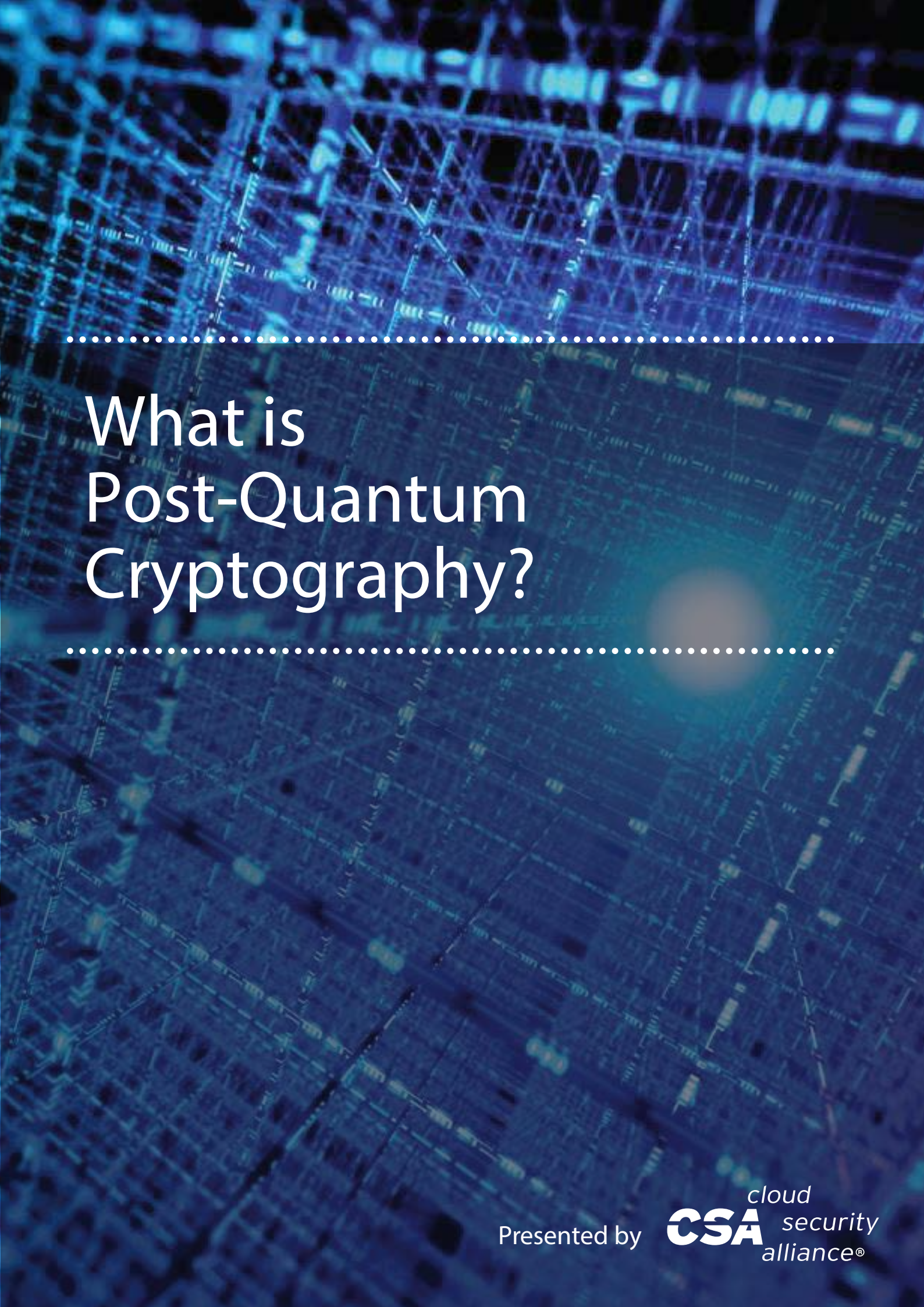


What is Post-Quantum Cryptography?

Presented by CSA cloud security alliance®

Acknowledgments

Quantum-Safe Security working group

Gene Carter
Don Hayford
Bruno Huttner

Cloud Security Alliance

Hillary Baron
Frank Guanco
JR Santos
John Yeoh
Aaron Dean
Ryan Bergsma

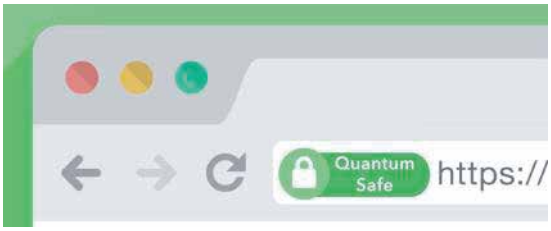
Special Thanks

Victoria Choi
Christoph Jaggi
Nino Walenta

What is Post-Quantum Cryptography?

Most people pay little attention to the lock icon on their browser address bar that signifies a secure HTTPS connection. They don't realize that there is an exchange of keys to assure that the communications are secure and a signature with the data to assure its integrity. But what if that connection cannot be trusted? The impact on the world economy could be devastating, as eCommerce, Cloud applications and storage, Online Stock Trading, and anything that relies on HTTPS would be rendered useless.

This scenario is possible in the not-too-distant future. Quantum computers will be able to break the current public key infrastructure that is the backbone of secure websites. Researchers at universities and corporations, as well as the NSA and the Chinese government, are all working to create a quantum computer with sufficient computing power to break the HTTPS connection. Thankfully, solutions exist today that can resist quantum computing attacks and avoid this economic Armageddon. In particular, there are several classes of new cryptographic algorithms, which are currently believed to resist quantum computer attacks. These are at the basis of post-quantum cryptography. However, the efforts to replace vulnerable asymmetric encryption and signing algorithms, including the ubiquitous RSA and ECC algorithms, need to begin several years before quantum computers are available if they are to be in place in time. It is necessary to start integrating post-quantum algorithms in cryptographic protocols today. The US National Security Agency (NSA) announced that it is planning to transition to a new cipher suite (Suite B) that is resistant to quantum attacks.[1]



Breaking Public Key Cryptography

Current secure HTTPS communications rely on an exchange of keys generated by asymmetric cryptography to ensure that the parties are who they say they are. Once these keys are exchanged, the data is then encrypted with symmetric cryptography, such as AES, and signed with asymmetric cryptography, like RSA.

In 1994, a mathematician named Peter Shor, developed an integer factorization algorithm that runs on a quantum computer. Shor's Algorithm[2], as it is known, can find prime factors for a given integer substantially faster than with the most efficient conventional factoring algorithm.

So a quantum computer with a sufficient number of qubits running Shor's algorithm could be used to break asymmetric public-key cryptography schemes such as the widely used RSA and ECC schemes.

Popular symmetric algorithms, including AES, are not broken by Shor's Algorithm. However, another method, called Grover's Algorithm[3], will effectively cut the security levels in half. For example, AES-256 will be rendered only as secure as AES-128 by running Grover's Algorithm on a sufficiently strong quantum computer. So post-quantum symmetric cryptography does not need to be changed significantly from current symmetric cryptography, other than by increasing current security levels.

Key Exchange and Digital Signatures

There are two crypto processes that utilize asymmetric cryptography: Key Exchange and Digital Signatures.

Key exchange is the method by which keys are exchanged between two parties. If the sender and receiver want to exchange encrypted messages, each must be able to encrypt and decrypt messages, which are generally done by a symmetric key cipher and requires both parties to have a copy of the same key. The exchange of that symmetric key is handled by Public key infrastructures (PKIs) in which each user applies to a 'certificate authority' for a digital certificate which serves as an authentication of identity.

The current danger facing key exchange is that organizations are able to record internet data today and decrypt it at a later date, once they are able to break the asymmetric algorithm (through Shor's algorithm, for example). Quantum Safe Cryptography can address this Store and Decrypt attack now within existing PKIs.

Digital signatures employ asymmetric cryptography to give the receiver trust that the message was sent by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for financial transactions, contracts, software patch distribution, and other cases where trust is important.

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 your computer.

The Alternatives

The advent of quantum computing does not mean that cryptography is dead. There are several classes of cryptographic systems that are currently believed to resist quantum computing, including:

- Lattice-based cryptography. Lattice supports digital signatures and key exchange. The most well-known example being NTRU[4] and NTRU MLS.
- Multivariate-quadratic-equations cryptography. Typically only signatures are supported. Hidden Field Equations (HFE)[5] is an example of this class of cryptography, as is the Rainbow (Unbalanced Oil and Vinegar)[6] scheme.
- Hash-based cryptography. Typically only signatures are supported. Hash-based requires hash trees in combination with one time signatures called the Merkle[7] signature scheme.
- Code-based cryptography. Code-based supports key exchange and it is currently not practical for signing. Examples of code-based crypto are McEliece[8] and Niederreiter[9] cryptosystems and their variants such as PQGuard[10], Wild McEliece[11] and McBits[12].
- Supersingular Elliptic Curve Isogeny Cryptography[13]. Typically only supports encryption. This cryptographic system creates a Diffie-Hellman type replacement with forward secrecy.

For the most part, post-quantum cryptography can function as a drop-in replacement to legacy cryptography, with some differences. One drawback of many post-quantum cryptography algorithms is that they require larger key sizes than current popular public key algorithms. However, some schemes already have performance levels comparable to, or even significantly better than pre-quantum algorithms. In addition, one can expect that, with additional attention paid to these new schemes, they will improve rapidly. As key size, computational efficiency and signature size all impact the performance of a system, making a comparison between solutions is difficult. The best post-quantum crypto solution for an application that continually transmits large amounts of signed data may not be the best choice for a different application that sends only a few bytes intermittently.

In order to facilitate the transition, an intriguing solution, maybe slightly more costly in terms of resources, is to encapsulate the current methods into the new ones. This will provide a solution, which is as safe as the best of both methods. An example of this is the proposed Quantum Safe Hybrid ciphersuite being considered by the IETF[14]. Thanks to the continuous increase in computing power, the overhead generated by this solution should not be a major hurdle.

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 the 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 3rd party. The key is then used with conventional symmetric encryption or authentication techniques. QKD has been explained inter alia in a previous whitepaper published by the Quantum-Safe Security Working Group. It is likely that both QKD and Post-quantum algorithms will find their applications in the future post-quantum cryptographic world.

References

[1] NSA website https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[2] Peter W. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. (Jan 1996)

[3] Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996)

[4] Security Innovation website www.securityinnovation.com/NTRU

[5] Nicolas T. Courtois: The security of Hidden Field Equations (HFE), http://hfe.minrank.org

[6] Jintai Ding and Dieter Schmidt: Rainbow, a New Multivariable Polynomial Signature Scheme (Dec 2014)

Ralph C. Merkle: A Digital Signature Based on a Conventional Encryption Function (Dec 2000)

[7] R.J. McEliece: A Public-Key Cryptosystem based on Algebraic Coding Theory, DSN Progress [8] Report 42-44:114 (Jan-Feb 1978)

[9] H. Niederreiter: Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory 15 (Jan 1986)

[10] Post-Quantum website: https://post-quantum.com/pqguard

[11] D. J. Bernstein, T. Lange and C. Peters: Wild McEliece Incognito, Lecture Notes in Computer Science vol. 7071 pp. 244-254, 2011

[12] D. J. Bernstein, T. Chou and P. Schwabe: McBits: Fast Constant-Time Code-Based Cryptography, Lectures in Computer Science vol. 8086 pp. 250-272, 2013

[13] Luca De Feo, David Jao, and Jerome Plut: Towards Quantum-resistant Cryptosystems from Supersingular Elliptic Curve Isogenies

[14] William Whyte: IETF website https://tools.ietf.org/html/draft-whyte-qsh-tls12-00

The permanent and official location for Cloud Security Alliance Quantum-Safe Security research is https://cloudsecurityalliance.org/group/quantum-safe-security/.