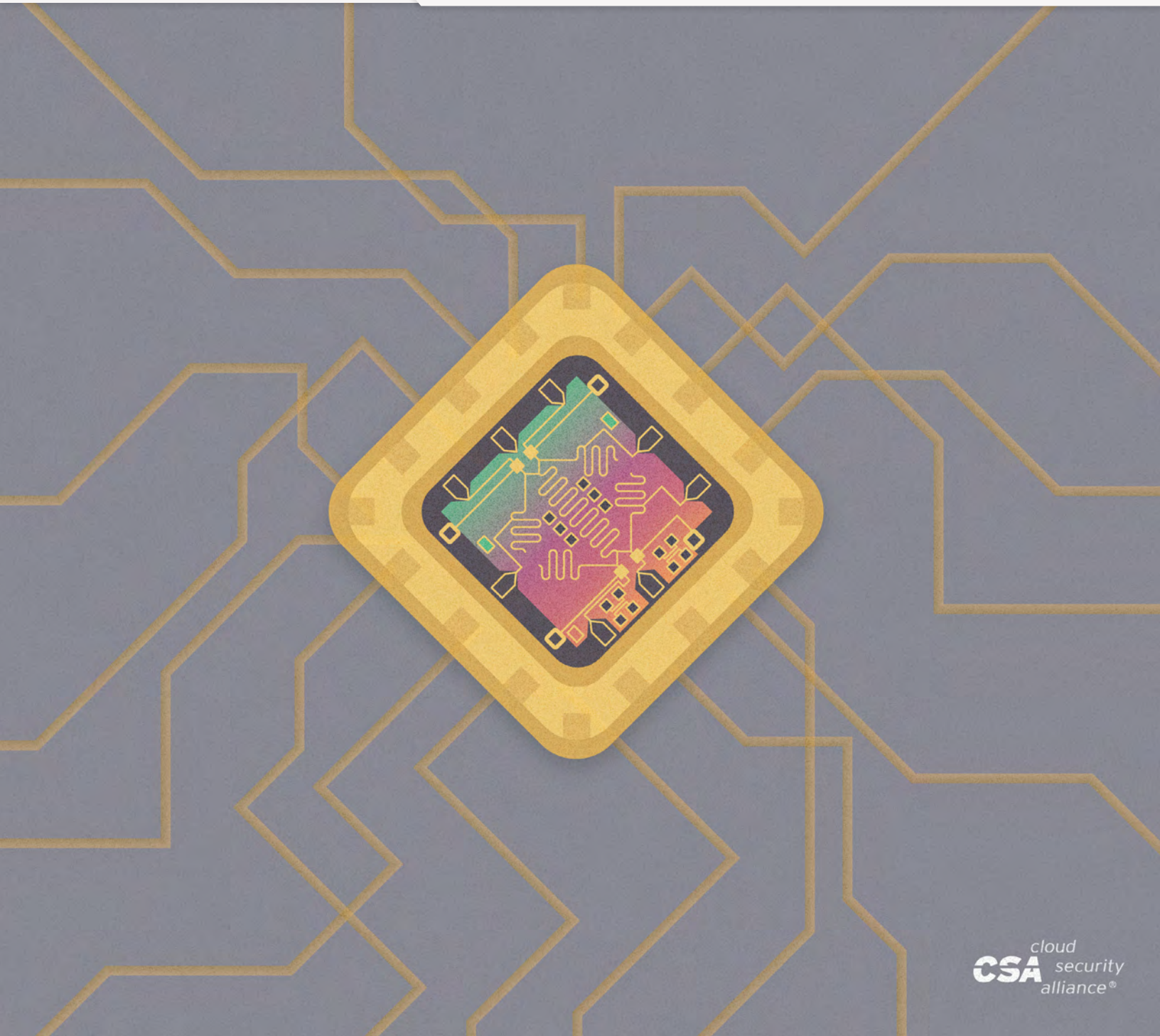
Quantum-Safe Security Working Group Glossary



cloud security alliance®

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

Acknowledgements

Cloud Security Alliance
Frank Guanco
Ryan Bergsma
Victor Chin
Stephen Lumpe

Quantum-Safe Security Working Group
Bruno Huttner, *Co-Chair*
Jane Melia, *Co-Chair*
Gene Carter
Ludovic Perret
Lee Wilson

The Quantum-Safe Security (QSS) Working Group was formed to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting networks and data. The working group is focused on long-term data protection amidst a climate of rising cryptanalysis capabilities. This glossary is a collective contribution of the QSS Working Group to increase quantum-safe security awareness, and includes a compilation of common terms used in the world of quantum-safe cryptography. However, quantum-safe cryptography is a very dynamic issue, prone to unpredictable patterns and instability. In anticipation of these characteristics, the QSS Working Group plans to update this document from time to time moving forward.

BQP

The class of problems that can be efficiently solved by quantum computers is called BQP (bounded error, quantum, polynomial time). Quantum computers only run probabilistic algorithms, so BQP on quantum computers is the counterpart of BPP (bounded error, probabilistic, polynomial time) on classical computers. BQP is defined as a set of problems solvable with a polynomial-time algorithm, whose probability of error is bounded away from one half. A quantum computer is said to "solve" a problem if, for every instance, its answer will be correct with high probability. If that solution runs in polynomial time, then the problem is in BQP. It is suspected that no Non-deterministic Polynomial-time hardness (NP-hard) problems exist in BQP.

CFS

This is a code-based signature scheme designed by N. Courtois, N. Sendrier and M. Finiasz in 2001 [CFS01].

Closest Vector Problem (CVP)

The Closest Vector Problem is Non-deterministic Polynomial-time hardness (NP-hard) and requires the closest vector of a given vector to be found in a lattice. This is a hard problem that occurs in lattice-based cryptography.

Code-based cryptography

This is a sub-area of quantum-safe cryptography and includes cryptographic schemes whose security is related to the computational hard problem of decoding linear error-correcting codes.

D-Wave machine

This is the first quantum machine publicly available (from D-Wave Systems, Canada). The machine is not a general purpose quantum computer, but instead is targeted at quantum annealing.

Entropy source

The combination of a noise source—such as a Quantum Random Number Generator, health tests and an (optional) conditioning component—to produce full-entropy random bits [NIST].

Grover's algorithm

This is an algorithm named after L.K. Grover [Grover96]. The algorithm provides a quadratic speed-up for an exhaustive search on quantum computers. It was designed as a database search algorithm, but can be used to reduce the cryptographic strength of symmetric algorithms by half.

Hash-based cryptography

This is a sub-area of quantum-safe cryptography which refers to signature schemes whose security are based on the hardness of finding a collision in a hash-function. The signature schemes are usually constructed by combining a one-time signature scheme or few time signature scheme with a Merkle tree. Some examples are the Leighton-Micali scheme [LM], SPHINCS [SPHINCS], and XMSS [XMSS].

Hidden Field Equations (HFE)

This is multivariate public-key scheme (encryption and signature) proposed by J. Patarin [HFE] in 1996. HFEv- [PCG01] is a secure variant of HFE which only permits a signature that can not be utilized to encrypt data.

Information-theoretic secure

A cryptosystem is information-theoretically secure if its security derives purely from information theory. That is, the cryptosystem cannot be breached even when the adversary has unlimited computing power. Examples of information-theoretically secure cryptosystems include the classical one-time pad and Quantum-Key Distribution (QKD).

Isogeny

This is a particular type of mapping between two elliptic curves.

Isogeny-based cryptography

This is a sub-area of quantum-safe cryptography that constructs public-key schemes whose security is dependent on the difficulty of recovering an unknown isogeny between a pair of elliptic curves. An example is the scheme of D. Jao and L. De Feo [JF].

Lamport one-time signature scheme

This is the scheme that inspired hash-based signature scheme. The technique proposed by L. Lamport [LamportRR] requires a one-way function and can be used to sign, at most, one message.

Lattice-based cryptography

This is a sub-area of quantum-safe cryptography and includes cryptographic schemes whose security is related to the Closest Vector Problem (CVP), the Learning with Errors (LWE) problem or the Shortest Vector Problem (SVP).

Learning with Errors (LWE) problem	This is a hard problem used in lattice-based cryptography. The solution to the problem, an issue introduced by O. Regev [Reg05], requires the recovery of a noisy linear equations system.
McEliece encryption scheme	This is a code-based public-key encryption scheme proposed by R.-J. McEliece in 1978 [McE78].
Merkle tree	This a data structure named after R. Merkle [Merkle89] that is also known as a hash tree. It is a binary tree whose leaves are blocks of data which are hashed and then combined with other blocks through hashing. This hashing combination is repeated until all blocks have been combined into a single hash.
Merkle Tree Signature Scheme	This is a typical example of a hash-based signature proposed by R. Merkle. The scheme's principle is to use a Merkle tree whose leaves are the public/private keys of a one-time signature. This allows the Lamport one-time signature scheme (or other one-time or few-time signature schemes) to be extended for signing more than one message. The number of messages that can be signed depends on the height of the Merkle tree. The signature scheme requires a collision-resistant hash-function or a pre-image-resistant hash-function.
Multivariate-based cryptography	This is a sub-area of quantum-safe cryptography which includes cryptographic schemes whose security is related to PoSSo problem or Multivariate Quadratic (MQ) problems. This problem is also called an MQ problem when the non-linear equations are of degree (at most 2) and remains NP-hard.
Multivariate Public-Key Cryptography (MPQC)	This refers to public-key multivariate cryptosystems.

Multivariate Quadratic (MQ) problem	This is a restriction of the PoSSo problem to quadratic polynomials.
Noise Source	A system the produces non-deterministic random numbers. The noise source contains the non-deterministic, entropy-producing activity [NIST].
Non-deterministic Polynomial time (NP)	This is a complexity class of decision problems in which affirmations (occurrences where the answer is "yes") can be verified in deterministic polynomial-time.
Non-deterministic Polynomial-time Hardness (NP-Hard)	Computational problems can be classified in function of their (intrinsic) hardnesses. NP-hard problems are at least as hard as the hardest problem in Non-deterministic Polynomial time (NP). An efficient algorithm for solving any NP-hard problem would lead to an efficient algorithm for all problems in NP. A fundamental assumption of quantum-resistant cryptography is that no NP-hard problem can be solved in deterministic polynomial-time in the classical and quantum setting.
NTRU	This is a patented and open-sourced lattice-based cryptosystem used to encrypt and decrypt data. It was developed by J. Hoffstein, J. Pipher, and J. H. Silverman [HPS98]. The signature scheme pqNTRUsign is based on the same underlying hard problem as NTRU and is also quantum-resistant.
PoSSo problem	This is the Non-deterministic Polynomial-time hardness (NP-hard) problem of solving a set of non-linear equations.

Post-quantum cryptography	This refers to the set of cryptographic schemes which will remain secure even in a world where quantum computers exist. This includes quantum cryptosystems such as Quantum-Key Distribution (QKD); algorithmic-based cryptosystems such as lattice-based, code-based, multivariate-based, hash-based and isogeny-based cryptosystems; and symmetric key cryptographic systems such as AES. Terminology related to post-quantum cryptography appeared in academic literature soon after P.W Shor's quantum polynomial-time algorithm for solving integer factorizations and discrete logarithm was introduced. Note that there remains some ambiguity around this term, with some organizations not including QKD.
Quantum annealing	This is a quantum process that solves optimization problems faster than if utilizing a classical computer.
Quantum bit or Qubit	This is the quantum analogue of a classic computer bit. It is a quantum system consisting of two levels, usually denoted by |0> and |1>.
Quantum computer	This is a computer that uses quantum-mechanics properties to perform computations. A quantum computer experiences exponential speedup in comparison to current computers on certain problems.
Quantum-computing resistant cryptography	A variant of quantum-resistant cryptography used recently by the International Organization for Standardization (ISO).
Quantum cryptography	This refers to cryptosystems whose security is guaranteed by the physical law of quantum mechanics. It differs from classical public-key cryptography, whose security relies on the difficulty of solving certain mathematical problems.

Quantum-Key Distribution (QKD)

Quantum-Key Distribution is an example of quantum cryptography that allows the information-theoretically secure distribution of keys between two spatially separate parties who are also connected by an insecure optical channel. There are two complementary approaches to QKD: (1) discrete variable quantum key distribution (DVQKD) uses single-photons or weak coherent states and single photon detectors; and (2) continuous variable quantum key distribution (CVQKD), which uses coherent or squeezed states of light and homodyne detectors. Both continuous and discrete approaches have been experimentally demonstrated; just as importantly, both have been proven to be information-theoretically secure.

Quantum Random Number Generator (QRNG)

This refers to quantum-based noise source that derives random numbers from measurements conducted on a quantum process or quantum system. The uniqueness and randomness of these measurements/outcomes are of quantum origin, as described by quantum mechanics. Examples of QRNGs include several commercial systems that generate random numbers from measurements made on optical quantum states of light.

Quantum-resistant cryptography

This term also refers to the set of cryptographic schemes which will remain secure even in a world where quantum computers exist. This terminology was used by the United States National Security Agency in their announcement regarding their, "preliminary plans for transitioning to quantum resistant algorithms." This term is not completely equivalent to post-quantum cryptography, as it only refers to algorithmic techniques. Additionally, it does not appear to include physical technology such as Quantum-Key Distribution (QKD).

Quantum-safe cryptography

This refers to the set of cryptographic schemes which will remain secure even in a world where quantum computers exist. The term was recently coined, but is often used interchangeably with the term "post-quantum cryptography." Furthermore, it has been used by working groups in the European Telecommunications Standards Institute (ETSI) and the Cloud Security Alliance (CSA).

Ring-LWE (RLWE) problem

This is a variant of the Learning with Errors (LWE) problem in which the (noisy) linear system to be solved is structured [LPR].

Shor's algorithm

This refers to the P.W. Shor algorithm [Shor], published in 1994, which allows integers to be factored and to find discrete logarithms in polynomial-time on a quantum computer. By using Shor's algorithm, most of today's commonly used asymmetric cryptosystems can be broken.

SVP

This stands for the Shortest Vector Problem, which requires the shortest vector in a lattice to be found. The problem is Non-deterministic Polynomial-time hardness (NP-hard) under randomized reduction for the Euclidean norm. This is a hard problem that occurs in lattice-based cryptography.

Syndrome decoding

This is a Non-deterministic Polynomial-time hardness (NP-hard) problem that occurs in code-based cryptography. The goal is to find a constrained solution of a linear system; that solution must have a small number of non-zero components.

Unbalanced Oil and Vinegar (UOV)

This is a multivariate signature scheme which was proposed in 1999 by A. Kipnis, L. Goubin and J. Patarin [KPG99].

Bibliography

[SPHINCS] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe and Z. Wilcox-O'Hearn. *SPHINCS: Practical Stateless Hash-Based Signatures*. EUROCRYPT 2015.

[XMSS] J. Buchmann, E. Dahmen, and A. Hülsing. *XMSS - a Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions*. Post-Quantum Cryptography, 2011.

[CFS01] N. Courtois, M. Finiasz, and N. Sendrier. *How to Achieve a McEliece-Based Digital Signature Scheme*, ASIACRYPT 2001.

[Grover96] Lov K. Grover. *A Fast Quantum Mechanical Algorithm for Database Search*. STOC 1996.

[JF] D. Jao and L. De Feo. *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*, Post-Quantum Cryptography 2011.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. *NTRU: A Ring-Based Public Key Cryptosystem*. ANTS-998.

[KPG99] A. Kipnis, J. Patarin, and L. Goubin. *Unbalanced Oil and Vinegar Signature Schemes*. EUROCRYPT'99, LNCS 1592, pages 206–222. Springer, 1999.

[LamportRR] L. Lamport. *Constructing Digital Signatures from a One Way Function*. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

[LM] F.T. Leighton and S. Micali. *Large Provably Fast and Secure Digital Signature Schemes based on Secure Hash Functions*. US Patent 5,432,852, July 11, 1995.

[LPR] V. Lyubashevsky, C. Peikert and Oded Regev. *On Ideal Lattices and Learning with Errors over Rings*. J. ACM, 2013.

[McE78] R.-J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114—116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[Merkle89] R. Merkle. *A Certified Digital Signature*. CRYPTO '89.

[HFE] J. Patarin. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*. EUROCRYPT'96.

[PCG01] J. Patarin, N. Courtois, and L. Goubin. *Quartz. 128-bit Long Digital Signatures*. CT-RSA'01.

[Reg05] O. Regev. *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*. STOC 2005.

[Shor] P. W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM J. Comput. 1997.

[NIST] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish and M. Boyle. *Recommendation for the Entropy Sources Used for Random Bit Generation (Second DRAFT)*. NIST Special Publication 800-90B, 2016.

