carahsoft.

Quantum Keyword Glossary

Quantum

Quantum Supremacy	Evidence demonstrating the superiority of quantum computers over classical computers, based on performance in tasks and outcomes.
Harvest-Now, Decrypt-Later	When protected data is intercepted today but only to be used/decrypted when a quantum computer can break the encryption.
Y2Q	"Years to Quantum" or "Years to Quantum Readiness" - referring to the estimated time until large-scale quantum computers become advanced enough to break current cryptographic systems and other public-key encryption methods widely used today.

Quantum Computing

Quantum computing	A cutting-edge area of computing that leverages the principles of quantum mechanics—the science that describes the behavior of particles at extremely small scales, like atoms and subatomic particles. Unlike classical computers, which use bits (representing 0s or 1s) as their basic unit of information, quantum computers use qubits (quantum bits). These qubits exhibit unique quantum properties such as superposition, entanglement, and quantum interference, enabling quantum computers to solve certain problems much faster than classical computers.
Quantum Gate-Based Computers (Universal Quantum Computing):	Universal quantum computing systems that use quantum gates to manipulate qubits, like how classical computers use logic gates. This approach enables them to perform complex computations across a wide range of applications, including cryptography, artificial intelligence, and quantum simulations. While highly promising, gate-based quantum computers require error correction and stable qubits to become scalable and practical for widespread use.

Quantum Annealers (Optimization-Focsed):	Specialized quantum computers designed to solve optimization problems by finding the lowest-energy state of a system. Unlike gate-based quantum computers, they use quantum fluctuations to explore possible solutions efficiently, making them ideal for logistics, scheduling, and machine learning tasks. While quantum annealers are commercially available today, they are not universal quantum computers and are primarily suited for combinatorial optimization rather than general-purpose computing.
Topological Quantum Computers (Fault-Tolerant Approach):	An advanced type of quantum computing that uses topological qubits, which rely on the braiding of exotic quasiparticles called non-Abelian anyons to store and process information. This approach makes them more resistant to errors compared to other quantum computing models, potentially enabling fault-tolerant quantum computing with fewer qubits. While still in the research phase, topological quantum computers could provide a scalable and stable foundation for future quantum applications.
Analog Quantum Simulators (Physics-Specific Simulations):	Specialized quantum devices designed to model and study specific quantum systems, such as molecular interactions, high-energy physics, and material science. Unlike universal quantum computers, they do not perform general-purpose computations but instead mimic real-world quantum behaviors to solve complex physics problems more efficiently than classical supercomputers. These simulators are particularly useful for drug discovery, fusion energy research, and quantum material design.
Qubits	The basic unit of quantum information, unlike classical bits, which are either 0 or 1, qubits can exist in a superposition of both states simultaneously, allowing for parallel computation.
Superposition	When qubits can exist in multiple states (both 0 and 1) at the same time, this enables quantum computers to process a vast number of possibilities simultaneously.

carahsoft

Quantum Keyword Glossary

Entanglement	When a phenomenon where qubits become linked, such that the state of one qubit instantly influences the state of another, regardless of the distance between them. This allows for highly correlated calculations and secure communication.
Quantum Tunneling	Exploits the ability of particles to pass through barriers, useful for detecting small energy changes.
Quantum Interference	When quantum computers use interference to amplify correct solutions while canceling out incorrect ones during computation.
Superconducting Qubits	Qubits made from superconducting circuits, used by IBM, Google, Rigetti.
Trapped Ion Qubits	Qubits made from ions trapped in electromagnetic fields, used by IonQ, Quantinuum.
Topological Qubits	Hypothetical qubits that encode information in braiding anyons, researched by Microsoft.
Quantum Noise	Unwanted disturbances that affect qubit stability and introduce errors.
Shor's Algorithm	Hypothetical qubits that encode information in braiding anyons, researched by Microsoft.

Quantum Security

Quantum Security	The field of cybersecurity that focuses on protecting data and systems from threats posed by quantum computing advancements.

carahsoft

Quantum Keyword Glossary

Quantum Cryptography	The use of quantum principles to secure communication, ensuring high levels of security.
Crypto Agility	The ability of an organization or system to quickly and easily switch between cryptographic algorithms and protocols without significant disruption to its operations, systems, or infrastructure. This concept is critical in ensuring long-term data security, especially in the face of evolving threats such as quantum computing or the discovery of vulnerabilities in existing cryptographic methods.
Lattice-Based Cryptography	A PQC approach that relies on complex mathematical lattice structures, used in Kyber and Dilithium.
Hash-Based Cryptography	Uses secure hash functions for quantum-resistant digital signatures, used in SPHINCS+.
Quantum-Resistant Encryption	Cryptographic methods designed to withstand attacks from quantum computers.
Quantum Key Distribution (QKD)	A secure communication method that uses quantum mechanics to share encryption keys.
Post-Quantum Cryptography (PQC)	Cryptographic algorithms designed to resist quantum computing attacks.
Quantum-Safe Encryption	Encryption methods that remain secure even in the age of quantum computers.

carahsoft

Quantum Keyword Glossary

Quantum Random Number Generator (QRNG)	A device that uses quantum mechanics to generate truly random numbers for cryptography.
Quantum Attacks	Exploits that use quantum computers to break classical cryptographic systems.
Quantum-Safe Algorithms	Algorithms like lattice-based cryptography, hash-based cryptography, and multivariate polynomials that resist quantum attacks.
Quantum Entropy	a concept that helps us understand how "random" or "uncertain" a quantum system is. It's like a measure of how much information we don't know about a system or how mixed up it is. In classical physics, entropy is used to describe disorder—like how jumbled up the molecules in a gas are. Quantum entropy takes this idea to the quantum world, where systems can be in strange states, like being in multiple configurations at once (**superposition**) or deeply connected (**entanglement**).
Quantum Sensing	a technology that leverages the principles of quantum mechanics, such as **superposition, entanglement,** and quantum tunneling, to measure physical quantities with extremely high precision and sensitivity. It uses quantum phenomena to detect or measure phenomena that are often undetectable or difficult to measure using classical sensors.