

PQC News

- ETSI QSC WG Publishes Technical Report on QSC Migration: <https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes>
- Scientists develop first quantum algorithm to characterize noise across large systems: <https://phys.org/news/2020-08-scientists-quantum-algorithm-characterize-noise.html>
- Google's Quantum Computer Achieves Chemistry Milestone: A downsized version of the company's Sycamore chip performed a record-breaking simulation of a chemical reaction <https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/>
- IBM Quantum Roadmap Predicting between 10 and 50 logical qubits by end of 2023:
 - https://techcrunch.com/2020/09/15/ibm-publishes-its-quantum-roadmap-says-it-will-have-a-1000-qubit-machine-in-2023/?guccounter=1&guce_referrer=aHR0cHM6Ly9zbGFzaGRvdC5vcmcv&guce_referrer_sig=AQAAADzYsWcuhkzZdnrakIA6verB3aUIJfPMrL1hmXVXJ1NkMuwlKw9krKbUkmpa6PU58HScPXXICUnSJuvHLI1EZWFqG yW 2ZTjOIXKOMOUF6e8lp64-nGjIP7kNDgMmrbGRn twMHiIND4-PcGNPwzF4zJBHsRywcEtYPf3RGHAa
- IonQ Unveils World's Most Powerful Quantum Computer: <https://ionq.com/news/october-01-2020-most-powerful-quantum-computer>
- US Launches National Quantum Initiative: <https://www.quantum.gov/> and publishes report:
 - <https://www.quantum.gov/wp-content/uploads/2020/10/QuantumFrontiers.pdf>
- NIST/NCCoE Workshop on Migrating to QSC: <https://www.nccoe.nist.gov/events/rescheduled-virtual-workshop-considerations-migrating-post-quantum-cryptographic-algorithms>
- Its also worth noting that the NSA has come out in support of lattices and hash-based signatures. They do not seem to like Rainbow very much (from their comments in the NIST/NCCoE workshop). <https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/>