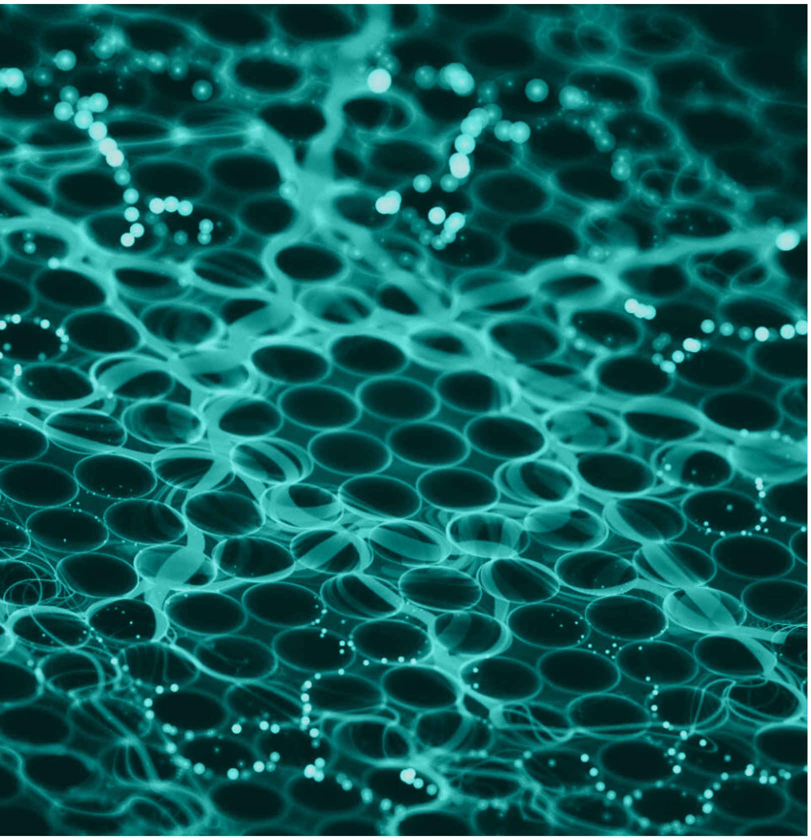
Embracing Our Quantum Future

By Ryan Hagemann, co-Director, IBM Policy Lab & Zaira Nazario, Technical Lead, Quantum Theory, Algorithms, and Applications, IBM Quantum

The world is on the cusp of another computer revolution. It will be driven by the convergence of powerful technologies: high-performance computing, AI, and quantum computing.

Quantum computing is not simply a faster way of doing what today's computers do – it is a fundamentally different approach that promises to solve problems that classical computing can never realistically solve. It holds the promise to help humanity confront important challenges, from solving long-standing questions in science to overcoming obstacles in improving industrial efficiency. Working in conjunction with classical computers and cloud-based architectures, quantum computers could even be the answer to problems we haven't yet dreamed of. The opportunities for society and the economy are potentially limitless.



Quantum computing can help to expedite the response to future pandemics, ongoing health crises, and the proliferation of debilitating diseases affecting millions worldwide through vastly improved chemical simulations in drug discovery and development. It will be able to improve the simulation accuracy of computational fluid dynamics, allowing for lower-cost approaches to improved manufacturing design processes. It could aid in optimizing portfolio investment strategies, using advanced modeling techniques that can better analyze the behavior of complicated financial markets. But quantum computers also pose a challenge for one important area of digital life: encryption.

The Crypto Conundrum

As detailed in a recent essay from IBM Research, advances in quantum computing will eventually present a significant information security challenge. The world is already heavily reliant on cryptography to protect data and critical infrastructure, and as quantum computers become more ubiquitous, digital platforms that are designed and deployed today can increasingly be vulnerable without the concurrent development and adoption of quantum-safe encryption.

The world is still a long way off from quantum computers that could break today's widely-used cryptography. We already know how to perform encryption that is resistant to a quantum computer's attack. Yet such foundational quantum-safe algorithms are only the start. Many industry security standards and protocols need to be updated for these new algorithms, and advances in quantum computing will need to coincide with advances in quantum-safe cryptography to ensure data is secured now from future threats.

Preparing for Tomorrow by Future-Proofing in the Present

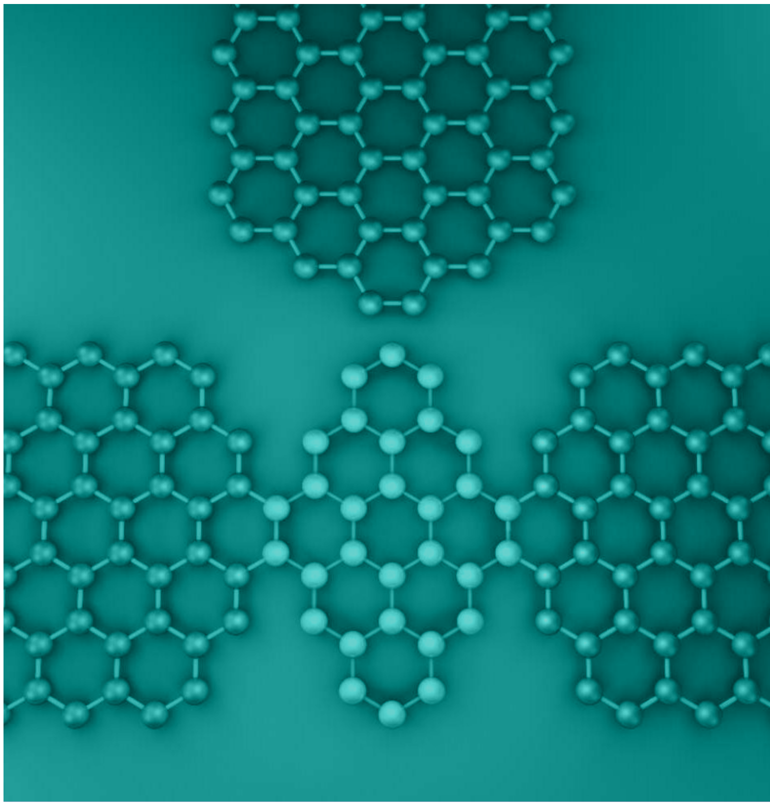
To prepare for what comes next, policymakers and industry need to look to mitigate against these risks by future-proofing in the present. We must act now.

IBM is. Our researchers are developing practical cryptographic solutions that are resistant to the threats posed by quantum computers. We have found a number of cryptographic schemes that are currently thought to be quantum-safe. These include lattice-based cryptography, hash trees, multivariate equations, and super-singular isogeny elliptic curves.

The key advantage of such quantum-safe schemes is the absence of exploitable structure in the mathematical problem an attacker needs to solve in order to break the encryption. Certain such quantum-safe schemes (e.g., supersingular isogeny) are future-proofed against particularly patient attackers who store their victims' encrypted messages today to decrypt them with more powerful methods in the future. Other schemes (e.g., lattice cryptography) can enable game-changing technologies like fully homomorphic encryption, in which data can be directly computed upon in its encrypted form, stymieing a common strategy of attackers today to loiter in a victim's computer system until sensitive data has to be taken out of encryption to perform computations upon it.

To advance these and other innovative new methods for securing data in an age of quantum computing, we are collaborating with academic institutions – such as the University of Waterloo and the University of Toronto – to advance the science behind these techniques. IBM is also engaging in global efforts to standardize quantum-safe cryptography. The most notable of these is the NIST PQC process. IBM has submitted a number of algorithms to the NIST PQC process and is working closely with other industry leaders in standard development organizations, such as ETSI, ISO and ANSI.

But governments have a role to play here too. To supplement private industry's engagement in standards development, governments need to accelerate investments in, and promote the adoption of, quantum-safe cryptographic schemes that can safeguard data now and long into the future.



Quantum Readiness

Forward-leaning companies and governments are preparing for a quantum computing future and positioning themselves ready to capture the many benefits of this technology. Yet, more can and should be done. Collaboration is key: governments, researchers, academics, and industry will need to work together on policies to accelerate the adoption of new educational curricula, fund R&D, create new talent pipelines, and more.

As governments look to lead in quantum computing, policymakers should consider the following recommendations:

Governments should recommend adoption of quantum-safe cryptography now to address future threats to data that is encrypted today.

Standard development organizations and their members should accelerate efforts around new quantum-safe cryptographic schemes and prioritize workstreams to establish a quantum-safe infrastructure. Government agencies, such as NIST, should take the lead in convening industries to agree on quantum-safe cryptographic standards, working with international partners.

Government agencies should accelerate the development of quantum computers through significant, sustained, and focused long-term investment in quantum information science to secure their nation's position at the forefront of the quantum computing race. Fundamental research in quantum theory, hardware, and software includes the development of novel qubits, methods to improve the quality of qubits and their performance in quantum circuits, techniques to mitigate and correct errors, development of optimized quantum circuits and compilation schemes, and components to enable the development of advanced scaling technologies.

Government agencies should support the rapid deployment of advanced, reliable quantum systems by being an early adopter to help drive developments and to enable an ecosystem of research, software and algorithm development, and commercialization. It is essential to promote industry uptake and experimentation and user-level ecosystem building in parallel to the efforts to advance the development of the hardware and systems themselves.

Governments must foster a collaborative framework involving national laboratories, academia, industry and international partners to advance the technology and build a competitive edge. Government, academia, and industry must work together to advance the fundamental science of quantum computing and execute an efficient and aggressive development roadmap with meaningful, well-defined metrics.

Governments should help build a robust enabling technology ecosystem and supply chain for the quantum industry and promote education and training of the necessary workforce to make the industry sustainable. Examples of initiatives to build up quantum industry supply chains include the Quantum Economic Development Consortium (QED-C) in the United States, and IBM's collaboration with Germany's Fraunhofer-Gesellschaft, Europe's leading organization for applied research.

Standard development organizations should prioritize the updating of system-relevant industry standards such as critical infrastructure and financial industry standards. The efforts should include updates to ISO 27001, COBIT, NIST SP 800-53, ANSI/ISA-62443, and standards developed by the Council on Cybersecurity Critical Security Controls.