Quantum Computing and Post-Quantum Cryptography

Waleed Yawer
Usama Nizamani
June 2021

POLICY BRIEF

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Executive Summary

Quantum computing is incrementally improving the overarching state of digital communication through the enhancement of machine learning and data decryption; which quantum computing is far more efficient in operationalizing than its traditional counterpart. While the latter is grounded in bit-based computing, modern quantum computers leverage quantum mechanics through 'qubits' as basic data units which can run millions of operations also termed 'gates' in a similar amount of time more efficiently than traditional computers. This enhanced ability to compute renders quantum computing both a conduit for digital enhancement transitioning into Web 3.0, as well as a challenge to be reckoned with if and when used to threaten a state's national security by disrupting encrypted messages and communications.

The following recommendations are proffered: -

- The Ministry of Information Technology and Telecommunication may want to build partnerships through MoU's with public and private sector universities to invest in quantum enabled software. Universities may use any funds allocated to improve their incubation and digital labs, offer courses with guaranteed job placements.

- The previous government in Pakistan announced a 'semi-conductor' zone with China's help. As important as this policy decision is, it is imperative that private digital organizations be taken on board as stakeholders and consultants in the development of semi-conductor zones. More currently, Pakistan needs to increase semi-conductor imports from China, if it is to enter digital partnerships with universities.

- The development of Quantum Labs is important for professionals to work on enhancing Pakistan's quantum capabilities in the commerce and communication sectors. Quantum labs will also facilitate a conducive digital environment for private organizations to work in.

- The Ministry of Information Technology and Telecommunication may want to create a pool of corporate entities that can benefit from quantum technology as important stakeholders for raising of capital. Such a pool can include organizations from the following sectors

    1. Banking
    2. Micro-Finance
    3. Automobile
    4. Trade and Commerce

Issue

Despite its benefits across various sectors, quantum technology can be used to disrupt communications which can have an adverse impact on national security. Furthermore, gauging each state's quantum capabilities, even with respect to more digitally able countries, is a cumbersome task given the nascency of the technology.

Analysis

Quantum-Computing and Commercial Applications

Quantum computing relies on use of combinatorics to solve complex problems, i.e. to figure the number of combinations by which a problem or different objects can be arranged. In any problem, where a number of items grow, the numbers of possible permutations grow exponentially also. The purpose of the combinatorics is to find a specific value through the process of high number of permutations. Classical computers programmed to calculate functions and programs between the binary of '0' and '1' are unable to perform computationally demanding task.[1] While the hardware of quantum computing remains in its infancy, progress remains underway to convert relative progress in area of quantum computing for commercial applications.[2] To this end, progress in quantum-enabled algorithms is facilitating solving of combinatorics on existing classical computers. Other than its application in cyber-security and developing quantum-resistant encryption or methods of decryption based on classical computing, quantum computing is under consideration for use includes: chemical engineering, and manufacturing sector.

The commercial market for quantum computing is expected to grow from $486.1 million to $3,180.9 million in 2028; an approximate increase of 554% which is indicative of the processing capability of quantum computers to benefit various sectors. By definition, artificial intelligence builds on a computer's interactive experience and digital proficiency to demonstrate 'intelligence', which by virtue of its ability to do so, brings forecasting into play.

Chemical Engineering

The discipline of chemical engineering requires use of combinatorics to figure possible combinations of atoms, and many possible ways that they can bond. At present, it is difficult to simulate classes of molecules by relying on classical methods; however, the possibility to run these simulations increases greatly due to improvements in the quantum computers. An existing company, OTI Lumionics, is already employing quantum technology to understand and determine structure of new molecules, especially its properties and structures jointly. Employing these approaches can allow researchers to use quantum-enabled algorithms for developments or breakthroughs in developments of drugs.[3]

[1] "Quantum Information," *Nature Magazine*, https://www.nature.com/subjects/quantum-information.
[2] Francesco Bova, Avi Goldfarb, and Roger G. Melko, "Commercial Applications of Quantum Computing," EPJ Quantum Technology 8, no. 2 (2021): 1-2, https://doi.org/10.1140/epjqt/s40507-021-00091-1.
[3] Bova, Gold Farb, Melko, "Commercial Applications," 2-3.

Manufacturing Sector

Equally as in the case of the chemical engineering, there is no major breakthrough in hardware, at scale, to operate major quantum solution. Solid State AI, another software company, has developed quantum-inspired classical algorithms by relying on classical computing infrastructure. The use of quantum-inspired algorithms is being used to reduce the incidents of process failure during manufacturing.[4] The purpose of these solutions is to increase return on assets in two different areas: first; profit margin; second, total asset turnover[5].

Aerospace Industry

Among the several non-military uses for quantum computing, Lockheed Martin an aerospace company with a market cap of $114.48 is investing significantly in enhancing operational efficiency of its aircrafts as well as expanding its portfolio into space exploration, through quantum computing. Lockheed Martin uses D-Wave Quantum computers to run preflight algorithms, reducing the probability of errors more efficiently than traditional computing algorithms.

Financial forecasting

Financial modelling is structured on an entity's ability to analyze market trends and measure growth patterns based on those trends. The use of quantum computing to predict market behavior with negligible error can help reduce volatility and the market manias, increase investor confidence and assist in more appropriate allocation of capital.

Contemporary applications of quantum technology

The United Kingdom recently announced the use of Distributed Ledger Technology (DLT) in a bid to help elevate crypto-assets into the mainstream banking and financial sector. DLT decentralizes financial transactions across various sectors that employ its use, decrypting each transaction through cryptography. Though the decryption is currently performed using traditional computing methods, the former is projected to become a major part of the formal business sector if quantum technology is used to compute transactions. Furthermore, quantum computing has shown utility in weather forecasting systems as well as enhancing institutional capacity for healthcare through investments in biochemistry.

Despite quantum computing's power to decrypt coded communication by running operations almost to the tune of millions simultaneously, its potential for advanced militaries to decrypt coded communication is nascent, yet in ascendancy. China and the United States are leading the world in quantum technologies with China having launched its first 'quantum satellite' in 2016 and the United States having invested in excess of $450 million into research and insights aimed at making inroads towards integrating quantum with traditional computing commercially by 2030.

The potential of cyber-attacks on critical infrastructure by Russia in the war in Ukraine, and a series of cyber-attacks on the American energy and social services infrastructure, leading to it

[4] Bova, Gold Farb, Melko, "Commercial Applications," 2-3.
[5] Total asset turn over refers to an organization's ability to efficiently use its assets.

has only exacerbated the need for transition, more urgently than initially predicted in American official circles.

Futuristic Outlook: Post Quantum Computing and Cryptography

Cryptography in traditional computing supposedly relies on the use of public-key encryption methods such as the RSA, which require multiplication of large prime number together for encryption. The traditional computing systems would need to "factorize the primes again,"[6] and as a consequence the procedure would take computers decades to perform decryption. Hence, the public key method until now was considered secure. An algorithm, at the theoretical level, for application in quantum-computing technologies has already been developed for quantum computers that would enable them to, "factorize large numbers into prime factors and crack asymmetric encryption in a matter of minutes."[7]

With significant finances and efforts invested in development of quantum-resistant encryption methods, there are numerous methods under study from the National Institute of Standards and Technology (NIST). These methods on the other hand would allow end-users to have quantum-resistant encryption. About 48 procedures, which are presumed to be quantum-resistant, are under review from the NIST. Among them a method termed as the Super singular Isogeny Diffie-Hellmann key exchange method (SIDH) is being considered among the most suitable ones.[8] The method is relatively less-memory intensive. Two-fold issues, at present, make their incorporation challenging: first; the computational effort and storage space requirements remain high; secondly, being in its technological infancy, its reliability remains under question.[9]

How could it Impact Communications and Defence

The use of quantum technology to exploit traditional encryption methods will certainly be disruptive: it will render the existing methods of encryption redundant. At present, NATO's Cyber Security Center is reported to have successfully deployed with post-quantum cryptography using Virtual Private Network (VPN). The solution was provided by a company called the

post-Quantum. The company relied on "Hybrid Post-Quantum VPN," technology, a solution comprising traditional encryption algorithms in combination with new post-quantum or quantum-resistant algorithms. The deployed technological solution is believed to be quantum-resistant.[10] With preparations gearing up for post-quantum cryptography, it appears NATO and United States of America are among the leading countries working on development of post-quantum cryptography or quantum-resistant cryptography. The NATO-US nexus is working on improving encryption-based communication at par with the disruptive potential of modern-day operational quantum computing, as well as using quantum technology to decrypt military

[6] Lily Chen et al., *Report on Post-Quantum Cryptography;* (National Institute of Standards and Technology, U.S. Department of Commerce, 2016), https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir_8105_draft.pdf.
[7] Lily Chen et al., "Report on Post-Quantum."
[8] Lily Chen et al., "Report on Post-Quantum."
[9] Lily Chen et al., "Report on Post-Quantum."
[10] Aaron Hurst, "NATO Successfully Tests Communication over Post-Quantum VPN," *Information Age*, March 2, 2022, https://www.information-age.com/nato-successfully-tests-communication-over-post-quantum-vpn-123498872/.

and intelligence communication from Russia. The prediction of American authorities of a Russian attack on Ukraine days before the deed was not an act in clairvoyance, but an effective gathering and analysis of intelligence. In that context, quantum computing will be a blessing for intelligence gathering during conflict, as well as conflict prone regions.

In the United States, Department of Homeland Security in conjunction with the National Institute of Standards and Technology is working with the NIST to develop standards to protect data of organizations and reduce risks that may result with breakthroughs in quantum computing technology.[11]

Geopolitical Implications

Geopolitically, bilateral and multilateral alliances are increasingly beginning to be shaped around intelligence sharing between allies as a measure of reducing trust deficit. AUKUS and the evolving dimensions of the US-India relationship point emphasize the need to share real time information into possible hostile moves in the planning by 'hostile' states. Hypothetically, were the power to harness quantum computing be realized between states with stronger and more advanced digital footprints, less digitally able countries including Pakistan with a comparatively underdeveloped and underfinanced digital infrastructure will have to tend to asymmetrical hybrid warfare. States and militaries with quantum capabilities will hold an invaluable advantage over their adversaries in direct or protracted conflict.

India's prowess in quantum technology is underdeveloped but not underfinanced. An Rs.8,000 Crore worth investment was appropriated for universities and professional digital spaces last September to enhance India's quantum footprint. The country does not have a robust domestic hardware producing industry, which is why the focus currently is on developing quantum resistant software. However, there is growing recognition in India for need to domestically produce in addition to the import of super conducting chips to boost quantum technology in India.

Measuring a country's use of quantum technology for defense communication in an environment wherein the focus of the former is on quantum-resistance and not quantum offensives is cumbersome. For now, states, wary of the quantum capabilities of their adversaries are investing in ramping up of quantum enabled digital software to be better prepared for any offensives by digitally powerful states.

Recommendations

- The Ministry of Information Technology and Telecommunication may want to build partnerships through MoUs with public and private sector universities to invest in quantum enabled software. Universities may use any funds allocated to improve their incubation and digital labs, offer courses with guaranteed job placements.

- The previous government in Pakistan announced a 'semi-conductor' zone with China's help. As important as this policy decision is, it is imperative that private digital organizations be taken on board as stakeholders and consultants in the development of semi-conductor zones. More currently, Pakistan needs to increase semi-conductor imports from China, if it is to enter digital partnerships with universities.

[11] "Post-Quantum Cryptography." *Department of Homeland Security*, October 5, 2021. https://www.dhs.gov/quantum.

- The development of Quantum Labs is important for professionals to work on enhancing Pakistan's quantum capabilities in the commerce and communication sectors. Quantum labs will also facilitate a conducive digital environment for private organizations to work in.
- The Ministry of Information Technology and Telecommunication may want to create a pool of corporate entities that can benefit from quantum technology as important stakeholders for raising of capital. Such a pool can include organizations from the following sectors

    1. Banking
    2. Micro-Finance
    3. Automobile
    4. Trade and Commerce