RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

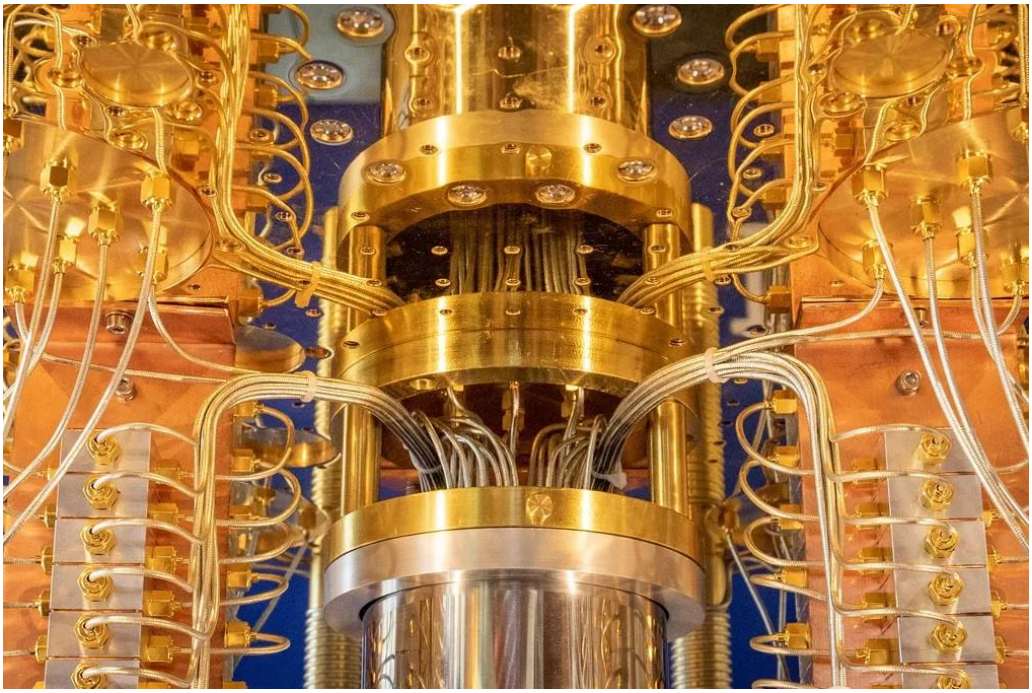
www.rsis.edu.sg No. 050 – 20 May 2022

Rethinking the 'Quantum Apocalypse'

By Shantanu Sharma and Manoj Harjani

SYNOPSIS

Proponents of an imminent "quantum apocalypse" – where quantum computers are sufficiently powerful to render current data encryption methods vulnerable – must reckon with the significant obstacles facing quantum computing. The issue ahead for policymakers will be to ensure a timely and sustainable transition to quantum-resistant encryption.



A close-up view of the IBM Q quantum computer. The processor is in the silver-coloured cylinder. Quantum computers are many times more powerful than current 'classical' computers.— CNET

COMMENTARY

EARLIER THIS year, the White House issued a memorandum mandating American government agencies transition relevant systems to quantum-resistant encryption. In a similar vein, the European Union allocated €11 million in 2022 to fund research on transitioning to quantum-resistant encryption.

Other countries are following suit. These efforts are motivated by the potential threat posed by quantum computers to current encryption methods that are widely deployed to secure data within communication protocols, authentication frameworks, and digital signing mechanisms.

Reassessing the Quantum Supremacy Race

Quantum computers harness the principles of quantum mechanics to perform calculations with qubits, in contrast to "classical" computers that rely on bits. With qubits, data can be represented by 0s and 1s at the same time, whereas bits are binary and can only represent data as 0 or 1. This allows quantum computers to solve certain types of computational problems more efficiently than classical computers.

Current encryption methods rely on the fact that certain computational problems cannot be easily solved by existing classical computers. However, once quantum computers eventually outperform the fastest classical computers for solving these challenging problems efficiently, any data secured by current encryption methods would be rendered vulnerable.

The timeline for a so-called "quantum apocalypse" therefore depends on a sufficiently powerful quantum computer being developed. To this end, many countries and companies are building increasingly advanced prototypes, leading to what some are describing as a race for "quantum supremacy", which in turn is raising fears of an imminent quantum apocalypse, potentially within this decade.

Although the competition to achieve quantum supremacy is an important development, it obscures the reality that merely outperforming classical computers alone is insufficient to cause a quantum apocalypse.

To break current encryption methods, considerably more powerful quantum computers are needed, and there are significant challenges to overcome as they are difficult to design, build, and operate. This primarily stems from the fact that quantum systems are easily disturbed by even the slightest interactions with their environment, such as a change in temperature.

Furthermore, a multi-year effort by the US National Institute of Standards and Technology (NIST) is seeking to develop standardised algorithms for quantum-resistant encryption. This is because there are currently several methods proposed that need to be evaluated and proven to be resistant to feasible attacks. NIST's quantum-resistant encryption algorithms are expected to be finalised between 2022 and 2024 and widely adopted globally.

Fighting Quantum with Quantum?

However, having standardised quantum-resistant encryption available does not mean the threat to data secured by current encryption methods is addressed entirely. NIST estimates that between five to 15 years are needed in a best-case scenario before the new quantum-resistant cryptographic standards will be sufficiently adopted.

This leaves a considerable window for malign actors to carry out cyber-attacks and steal data that could potentially be decrypted by quantum computers in future. A 2021 report by Booz Allen Hamilton argued that organisations should expect theft or interception of data with long-term intelligence value by Chinese actors. Nevertheless, any country developing quantum computers could potentially do the same.

As a result, some countries are concurrently developing new data protection methods using quantum technology, particularly to protect data with long-term intelligence value. Quantum key distribution (QKD) – which takes advantage of how sensitive quantum systems are to observation and interaction – is theoretically unbreakable even by a quantum computer, since it does not depend on the difficulty of solving a computational problem.

Several countries have invested in building and operationalising QKD networks, and China's efforts have been particularly ambitious. In 2016, China launched the world's first quantum communication satellite, and subsequently integrated this with an extensive ground-based network. Singapore too, has announced a multi-year project to build a National Quantum-Safe Network over the coming three years.

Like quantum-resistant encryption, however, QKD networks are still nascent and may not be as fool-proof as we think. The US National Security Agency, for example, has highlighted several potential limitations, including increased risks for denial of service, insider threats, and difficulties with validation and needing specialised equipment.

The Road Ahead

Technological answers to the quantum apocalypse in the form of quantum-resistant encryption and QKD networks are therefore not a silver bullet. Governments and companies will also have to address various organisational and operational issues that already pose a challenge for implementing traditional cybersecurity.

There will be a need to take stock of existing systems, assess future needs, and prepare organisations for an eventual transition to suitable countermeasures.

However, engaging in this process is likely to be out of reach for many smaller organisations, and governments will have to step in, particularly to safeguard companies involved in critical infrastructure and developing sensitive technologies. Furthermore, there will be a need to build the capabilities of information security officers and in-house cybersecurity teams.

In Singapore's case, it should build on the success of existing efforts to improve cybersecurity to get a head-start on managing the threat from a quantum apocalypse. Initiatives such as Cyber Security Agency of Singapore's Cybersecurity Labelling Scheme, as well as initiatives for certifications and to promote the use of pre-approved

solutions, could be expanded accordingly in tandem with focused engagement for strategically significant companies.

Indeed, Singapore's future as a digital nation and as a key player in quantum technology could well depend on its ability to achieve this transition. Investing in preparing organisations to secure their networks and systems using quantum-resistant encryption or QKD will arguably be as important as continuing to invest in advanced research and new quantum technology applications.

Shantanu Sharma is a Senior Analyst with the Centre of Excellence for National Security (CENS) and Manoj Harjani a Research Fellow with the Future Issues and Technology (FIT) research cluster at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg