

The revolution of quantum computing and its bearing on cyber security

July 2021

By Sony Anthony, Partner – Digital Trust (Cyber Security), KPMG in India

(4 min read)

Key takeaways:

- *Quantum Computing can be useful wherever there is a large, uncertain, and complicated system that needs to be simulated*
- *Been used successfully to deal with many challenges during the pandemic*
- *Methods for new commercial use of quantum computing cases in cybersecurity world*

Over the recent times, quantum physics has emerged as a promising problem solver in cases of small input with a vast array of possibilities in output. Industries across the globe are now realising the immense potential of quantum computing (QC) and the endless possibilities it offers for solving complex challenges.

QC can be useful wherever there is a large, uncertain, and complicated system that needs to be simulated. Use cases around QC, such as portfolio risk enhancement and fraud detection, weather prediction, deep learning and quantum cryptography have been around for some time. However, the COVID-19 crisis and the race to vaccine development has suddenly brought to focus the use of QC in drug discovery, development, and quantum tasks, such as genome sequencing. With all this happening around us, QC is expected to emerge as a game changer in solving future business problems as well.

Using quantum computing makes it possible to perform an operation in just a few seconds that would otherwise take years in a classical computer.

Researchers have used QCs to solve complex use cases during the current pandemic, such as:

- The modeling and simulation of spread of the virus
- The scheduling of nurses and other hospital resources
- Assessing the rate of virus mutation
- Adsorption of Remdesivir as an effective drug.¹

The possibilities are endless.

Quantum computing in cyber security:

¹Quantum mechanical studies of the adsorption of Remdesivir, as an effective drug for treatment of COVID-19, on the surface of pristine, COOH-functionalized and S-, Si- and Al- doped carbon nanotubes, NCBI, 4 February 2021

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

We know that QC is still in the nascent stage. However, in terms of cyber security, quantum computing has opened up possibilities both on the offensive and defensive side of things. According to a post quantum cryptography analysis, seven algorithms that may still be usable cryptographically after quantum computing becomes commercial have been finalised. This has led to new commercial use of quantum computing cases in cybersecurity world.

Quantum random number generator –

Random number generation is a key security element in cryptography today. It has applications in multiple areas across generation of seed keys, random passwords, OTPs, session keys and other trusted forms of communication.

The strength of key lies in the strength of entropy source used for generating the cryptographic keys.

Entropy as a Service (EaaS) –

The increase in IoT devices today and in critical infrastructure has resulted in organisations wanting to use secure cryptography without possibly having to configure or replace their infrastructure.

EaaS generates a seed that is provided to the local server or Public Key Infrastructure (PKI) setup to increase the randomness of the locally generated key. The EaaS server itself never saves the keys or gains knowledge of the ultimate key.

The generation of the seed via quantum cryptography requires expensive equipment. Therefore, EaaS helps organisations utilise the advantages of quantum cryptography without setting up costs.

Quantum Key Distribution (QKD) and key management –

The QKD mechanism takes the quantum key service a notch higher by allowing organisations to generate and manage their own quantum keys. In this model an organisation implements their own architecture to communicate and transmit secure keys over traditional channels.

This enables organisations to secure the keys in use while still leveraging the standard communication channels. In this way, even if the standard channel is compromised the keys are still secure.

How futuristic is this technology?

While this seems to be right out of sci-fi movies, the technology itself may be extremely close to commercialisation. In fact, there are cloud-based quantum computing services available and there are companies building commercial quantum computers.

This emerging technology is a boon to businesses no doubt; however, it comes with its own set of challenges. Going forward, businesses will need to focus on both the risks and opportunities that QC brings with it. To stay on top of the curve, the key is to have a well-planned strategy, with algorithms and existing systems to tackle the risks posed by quantum computing and capitalise on its endless opportunities.

For more information, refer KPMG in India's point of view titled: To qubit or not to qubit – is that the question?

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.