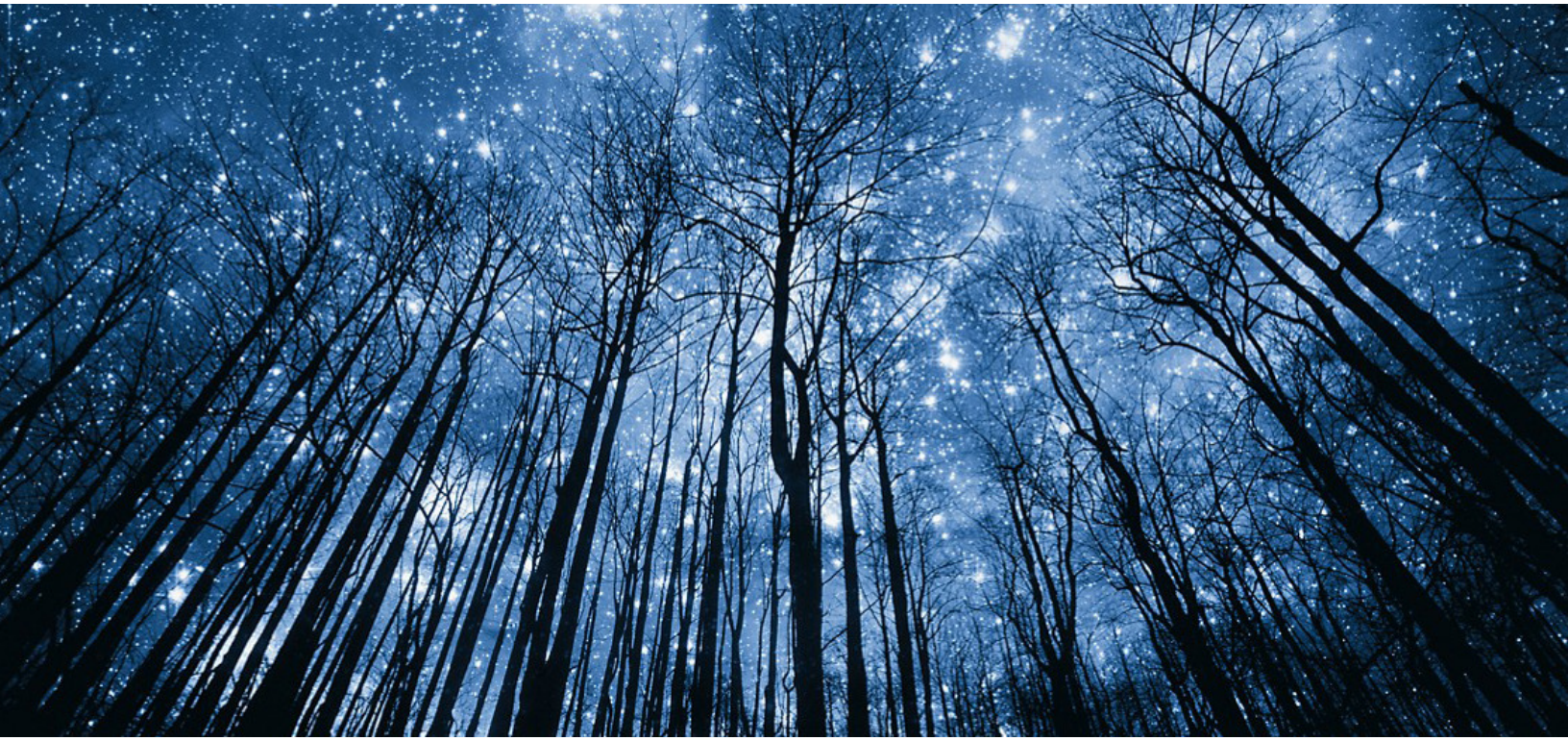
DELL Technologies

DATA PROTECTION IN A QUANTUM WORLD



Bharath Krishnan
Associate Sales Engineer Analyst
Dell Technologies
Bharath_krishnan@dell.com

Adil Ameen
Specialist 2, Inside Product
Dell Technologies
Adil_ameen@dell.com

Sunayana Devi
Associate Sales Engineer Analyst
Dell Technologies
Sunayana_devi@dell.com

Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Introduction

With the evolution of Quantum Computing, humanity learned about the paradigm shift that the potential of Quantum Mechanics could bring to their computational needs. Regular number-crunching operations that would typically require immense CPU and GPU processing power, could now be done in a much shorter time span if we could replace classical computers with quantum computers. Unlike classical machines that store and process data and information in the form of digital bits (0 and 1), quantum computers do so in the form of quantum bits or qubits, which can take the values 0 or 1, or a linear combination of both the states, represented by the probabilities of the qubit existing in one of them. Hence, increasing the number of qubits would allow calculations to be performed on all the states simultaneously, thereby exponentially scaling the power of compute. This property is termed as Quantum Superposition. In a world striving to increase data transmission speeds, qubits have the capability to transfer information between one another almost instantaneously, regardless of the distance between them, by a property called Quantum Entanglement.

Replacing conventional circuits with these sophisticated quantum circuits clearly add advantages to our compute requirements. However, these efficiencies come with a cost. Qubits are known to be intrinsically unstable and isolating them to reduce their degradation adds a lot of expense. Reducing the noise produced with increasing qubit count is another challenge that needs to be addressed. Assuming all the technical requirements to run a quantum computer have been met, we would then have to worry about the logical and ethical implications that it could produce. A machine of such capabilities would be able to break down heavily encrypted digital cryptography systems, introducing a new era of cyberattacks, all on a quantum level.

This article discusses this exact point, beginning with a brief introduction on quantum computing and what makes it a necessity despite its complexities. Beyond this, we discuss the possibility of quantum computers becoming a double-edged sword that could massively disrupt the data protection industry as it exists today. Are quantum computers of the future a boon… or a bane?

Quantum Mechanics

Quantum Mechanics is the field of modern physics that deals with the nature of matter at a microscopic scale. It studies and describes how the behavioral traits of the different things around us can not only change but completely go against the rules defined by classical mechanics or in other words, general laws of physics. The idea is to define a more generic governing body of physics that can be used to describe the properties of light and matter at both a microscopic and a macroscopic scale. Although quantum mechanics might seem like a poor substitute for classical mechanics, it is actually a more refined all-inclusive version of it and classical mechanics would eventually seem to be nothing more than just an approximation of the broader rules of quantum mechanics.

All quantities in quantum mechanics are defined by probabilities. This means, there will always be a level of uncertainty that limits the accuracy of values we measure on a quantum scale. If you're using the same technique to build a computer, you can assume how different the many fundamental aspects of the machine would look.

Qubits and Quantum States

A classical computer represents all data in the forms of bits – 0s and 1s. While a quantum computer follows a similar trend, it relies heavily on a game of estimates, as we discussed in the previous section. A quantum bit or qubit can also represent the values 0 and 1, but it would be characterized by the quantum state of that entity. In other words, it would represent the probabilities of the many outcomes of each measurement on the system. To put it even simpler, the quantum bit can exist as both 0 and 1 at the same time. This is called a linear combination of the two states, where we're trying to represent the probabilities using complex numbers.

Interference and Quantum Superposition

The concept of interference is as easy as that of simple arithmetic involving addition and subtraction. All things at a subatomic level tend to behave more like a wave rather than discrete particles. Which is why it is important to understand the concept of interference, which is the principle that explains how waves behave when they are superposed over each other. There are two kinds of interference – constructive and destructive. Constructive interference is when two waves combine to add up their amplitudes producing a wave of net greater amplitude. Destructive interference is when two waves combine to cancel out or negate their amplitudes, thereby producing a wave of net lower amplitude.

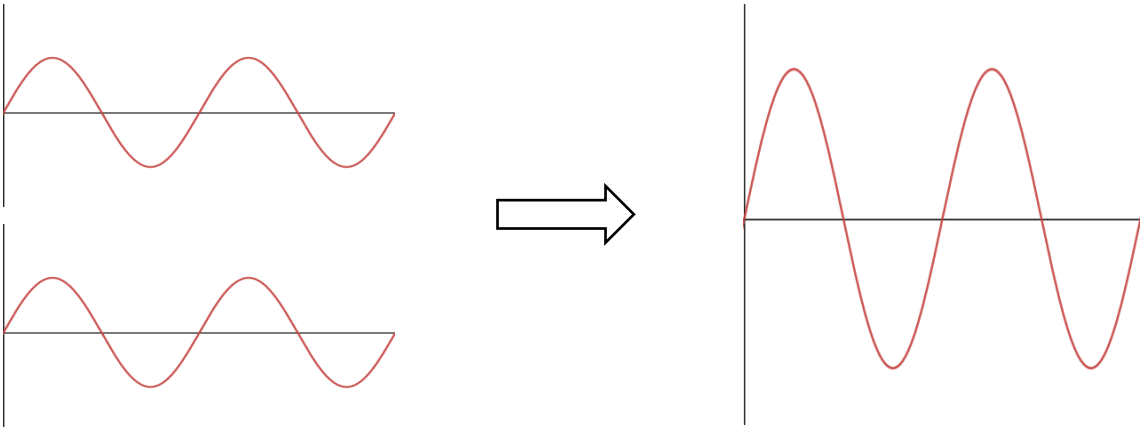


Figure 1: Constructive Interference – waves in phase add up.

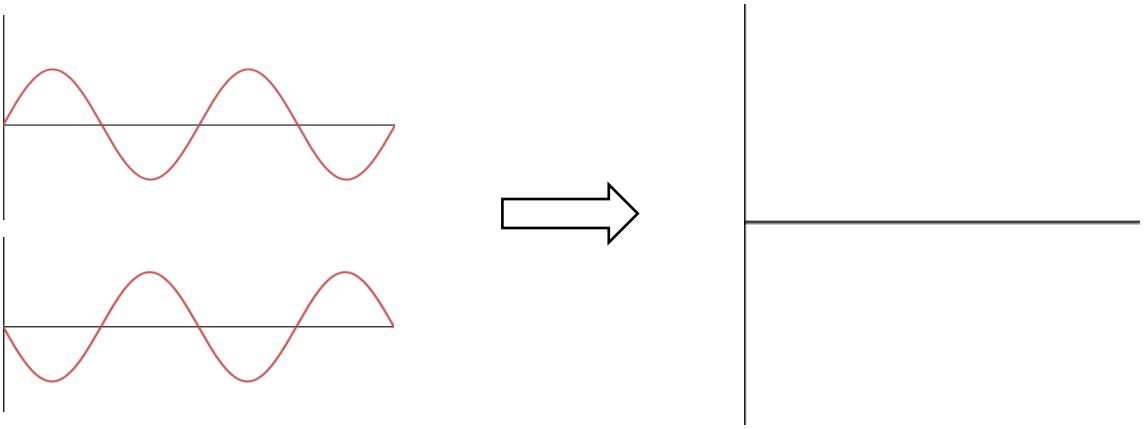


Figure 2: Destructive Interference – waves out of phase cancel out.

Fun Fact: The property of destructive interference shown in Figure 2 is what is generally used in noise cancelling headphones to reduce unwanted external noise from the environment. The headphones produce another wave that is approximately in the same range of frequency and amplitude as that of the external noise but superpose it out of phase over the original noise wave, thereby cancelling out most of it.

In a similar way, multiple quantum states can superpose resulting in interference or a combined state where both probabilities can exist at the same time. The property of a quantum system that allows it to exist in multiple quantum states simultaneously is called Quantum Superposition. A superposition of all potential computation states is first created and fed into a quantum circuit which uses a predetermined algorithm to selectively interfere the components of superposition. The final outcome of the quantum circuit is what is obtained after adding up and/or negating out the relative amplitudes and phases of the input state.

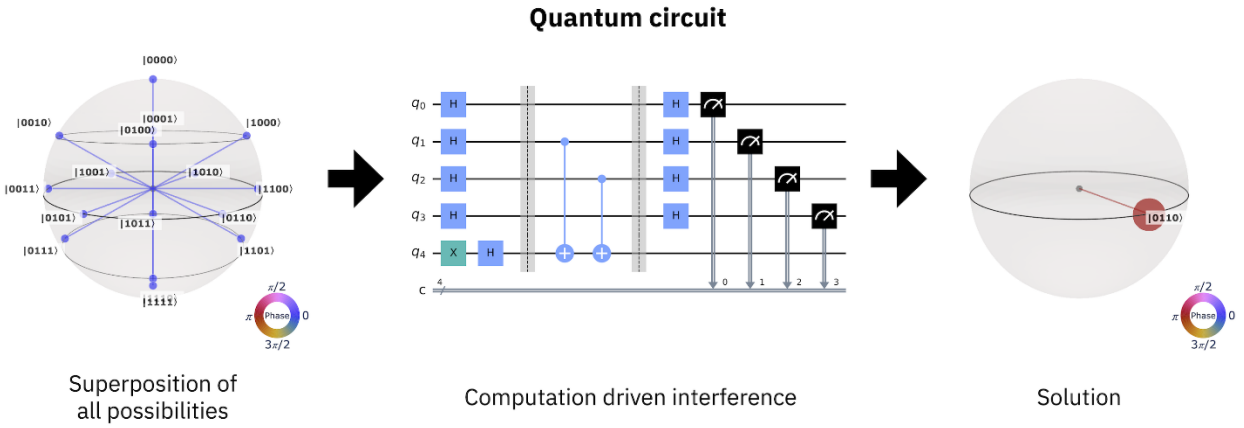


Figure 3: Quantum Computation by generating interference.

Quantum Entanglement

Another interesting phenomenon that can be used to great advantage in quantum computing is Entanglement; the quantum equivalent of the saying that the whole is greater than the sum of its parts, which means the combined state of qubits can bring a greater value than the independent qubits themselves. Two qubits, regardless of their physical proximity, have the ability to be entangled, by which they would then be defined by a common entangled state, where all of their physical properties would be perfectly correlated. These qubits can then be tweaked to transfer information from one qubit to the other, almost instantaneously. This is what is commonly referred to as Quantum Teleportation. Today, the logical upper limit to the data transfer speeds achievable my humankind is 299,792,458 m/s, which is the speed of light in a vacuum. But one day, even this limit might be eclipsed by the potential of Quantum Entanglement.

Threat to Cyber Security

The security of most of our data on any platform today depends on encryption. Although there are several different algorithms and encryption standards, most rely on a common strategy of sending information over a secure channel that is encrypted by a key or a pair of keys. In general, these keys might be used by a mathematical formula to scramble your data in a form that would make it non-identifiable by a third person who tries to eavesdrop on it. Popular encryption methods like RSA (Rivest–Shamir–Adleman) use a pair of keys; public key that is made available to the user and private key that is only available to the server. The public and

private keys are meant for encryption and decryption of data respectively and cannot be swapped for their purposes, thus securing the encrypted data from an attacker who manages to access it.

The private key is supposedly non-accessible because of the difficulty in cracking it. The mathematical formulation behind it is designed so that it takes a brute-force algorithm (trial-and-error approach that tries many potential keys to find a match) forever to find the right match. Ideally, we could change the keys periodically before an attacker finds it. The entire encryption system thus relies on the fact that there is no algorithm that can simply crack your keys fast enough. But this is only until the introduction of quantum computers.

Algorithms like the Schrödinger's Killer App algorithm are theoretically proven to run exponentially faster on a quantum computer. Using one such algorithm would drastically shorten the time it would take to crack a private key, thus making popular cryptography standards like RSA and ECC (Elliptic Curve Cryptography) extremely vulnerable to quantum cyber-attacks. For instance, an RSA key that would take trillions of years to be cracked by a classical machine, could be cracked in a few seconds by a large enough quantum computer of the future.

Data Protection in a Quantum World

What can we do about this possible disaster of the future that might disrupt the entire data protection industry? We're going to discuss two solutions to solve this problem, one that takes a software route and another that takes a more sophisticated hardware route. Both approaches are being heavily researched by public and private organizations around the world.

The first solution – **Post-Quantum Cryptography** – is purely based on improvising on the mathematical formulas that created the loophole for quantum computers to excel in breaking its encryption algorithms in the first place. It doesn't require any specialized hardware and relies completely on new mathematical challenges that are not vulnerable to quantum computing attacks. An important point to note is that quantum computers don't follow a brute force approach, but rather have algorithms that are made to leverage the different properties of qubits to perform more efficiently. This means, there is a selective number of problems that it can perform very well, and for the others, it'll just be as good if not worse, than a classical computer. Post-Quantum Cryptography aims to build a new standard of cryptography that is harder to crack, using both a classical machine and a quantum machine while still being as efficient and universally accessible as the existing standards.

The second solution – **Quantum Cryptography** – uses the laws of physics to build a new encryption system. This would demand specialized hardware that leverages the properties of quantum mechanics to reproduce the quantum equivalent of public and private keys for encryption. There are already quantum key distribution protocols like BB84 and E91 that are tested and proved to work under lab conditions. BB84 relies on a superposition-based approach, while E91 uses entanglement to exchange and validate its key pairs. Since it uses the fundamental laws of physics to secure data, it would require the attacker to literally break the very laws of nature first to break into the encryption. The only disadvantage is the requirement for sophisticated hardware, making it a less portable approach for wider use.

Conclusion

In essence, quantum computers would always be regarded as a double-edged sword. There might be several challenges that stand in our way to deploy and sustain an efficient quantum computer. Even after overcoming these difficulties to succeed in establishing something that is even remotely functional, we would then have to worry about the threats it would introduce if put into the wrong hands. However, as we learnt in the later section of this passage, the root cause of the problem itself is the solution to it. Despite the potential to break our systems today, we still invest heavily in learning, understanding and building a general-purpose quantum computer, all because the true potential of a quantum machine is yet to be explored. This will open doors of opportunity for us to influence the work we do and make it more efficient and accelerate growth at scale, while at the same time, introducing the possibility of mismanaged trouble that would then be the new challenge to solve.

Either way, humanity would keep learning.

"What we observe is not nature itself, but nature exposed to our method of questioning." ~ Werner Heisenberg

Bibliography

1. Is quantum computing the end of security as we know it? – TechBeacon
2. Is Quantum Computing a Cybersecurity Threat? – American Scientist
3. The Quantum Network Hacker Lab – Anastasia Marchenkova
4. Quantum Computing – IBM Research
5. Quantum computing and cybersecurity: How to capitalize on opportunities and sidestep risks – IBM
6. How Quantum Computing Will Transform Cybersecurity – Forbes
7. Quantum computing in a nutshell — Qiskit 0.37.1 documentation – Qiskit Development Team
8. Quantum computing will lead to new risks for cyber security – World Economic Forum
9. Protecting Our Data From Quantum Computers! | Post Quantum Cryptography – Anastasia Marchenkova (YouTube)
10. Will Quantum Computers break encryption? – Frame of Essence (YouTube)
11. Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D., 2022. *Report on Post-Quantum Cryptography*.