Entangling Quantum Computing

As we progress further into the era of quantum computing in relation to cyber security, there will be a particular word which will be used often and that word is called: “entanglement”. You see, quantum mechanics revolve much around the concept of “entanglement”.

Einstein called the concept as “spooky action at a distance” and was even mystified and unsure at such a phenomena initially. How could there be 100% and instant certainty about the properties (nature) of something very nearby or even at the other end of the universe?

Indeed, quantum computing is expanding a new frontier in physics called the entanglement frontier; unlike the frontier of small distances, eg, particle physics, or unlike the frontier of huge distances, eg, cosmology. Quantum entanglement is the process in which sub-atomic particles communicate with each other. It also helps to understand quantum algorithms.

A spooky situation

Particles are entangled when they are generated concurrently and at the same location. According to one Quantum theory, two electrons could maintain instantaneous communication, whether near each other or thousands of light years apart.

Moreover, a particle could be in more than one place at the same time! This is really spooky! Also, it deals with probabilities instead of certainties. The great mystery is that if one measures the electron, the other electron knows the other is being measured regardless of great distances between them.

Indeed, quantum entanglement is a mysterious event that happens when two particles (eg, sub-atomic particles) are linked, over great distances (always acting opposite to each other), in such a way that there is a correlation among the two particles; consequently, actions performed on one particle will immediately affect the other particles entangled with it.

In a quantum cryptographic situation, if you try to take action on one particle (if they are entangled), you’d instantly change the properties (nature) of the other; so attempting to hijack into the system would just destroy the encryption key (if there is one). Instantaneous communication

of quantum entanglement will lead us to further enhancing quantum cryptography.

Remember that quantum computing is about the use of quantum states of physical systems to store and transmit data, instead of the current "classical" states". The data could be processed and transmitted via the quantum measurement.

The current cryptographic security relies mainly on mathematics and some might say, the limited computing power.

To date, much deciphering of cryptographic codes are mainly a function of factoring extremely large numbers into prime numbers. However, quantum cryptography utilises photons and depends on the laws of physics rather than very large numbers and the deciphering of cryptographic codes in a quantum computing era could occur at the speed of light.

It should be noted that quantum cryptography to a great extent revolves around the "Heisenberg's Uncertainty Principle" propounded way back in 1927. Werner Heisenberg maintained that "it is impossible to determine simultaneously the exact position and momentum, (ie, mass X velocity) of a particle. ie, the more exactly the position is determined, the less known the momentum, and vice versa".

You may well ask: "What has this got to do with quantum computing?". Remember, the entanglement concept is one tool used in quantum computing, eg, in the use of transmitting data via entangled Qubit (which is a unit of quantum information that is stored in a quantum system). So if the position of the sub-atomic particle (read: data) is "uncertain", you may well ask: "Where exactly is the data then?".

I believe this is one of the great challenges in quantum computing! Remember, the Quantum Theory deals mainly in probability instead of certainty; it also focuses on physics rather than mathematics. And understanding the issue of entanglement is crucial in understanding quantum computing and/or quantum cryptography.

Leonard Yong, M.Acc, FCPA, CA, MACS(Snr), Convenor, CPA Cyber Security Forum Chairman, Digital Economy Committee, SHIREBIZ 22nd January 2019