The Quantum Leap
Guest Post by Harry Hannan
November 17, 2023

Demystifying Quantum Cryptography: Powers, Limitations, and the Path Ahead

Note: The following post was written by Quantum Leap guest contributor Harry Hannan of www.quantumpositioned.com

Quantum cryptography, sometimes also known as Quantum Key Distribution (QKD), sits at the intersection between the principles of quantum mechanics and traditional computational cryptography.

While Quantum computers have the potential to unlock today's secure communication, breaking almost all current encryption and unleashing a cryptographic apocalypse, quantum cryptography, in contrast, exploits the somewhat mind-boggling properties of quantum mechanics to protect data from quantum eavesdropping.

Standard Cryptography vs. the Quantum Computer

Over 90% of all standard cryptography relies simply on the fact that classical computers cannot factorise large numbers in any reasonable amount of time. This type of cryptography is known as RSA (Rivest-Shamir-Adleman) encryption and works because a classical computer would need to test all potential divisors one by one.

Shor’s algorithm is a quantum algorithm, developed by mathematician Peter Shor in 1994, which demonstrates a clear advantage of quantum computers over classical methods for solving these types of problems. It does this by taking advantage of qubits (see prior post here) and superposition (prior post here) being able to explore multiple potential divisors simultaneously. This leads to an exponential speedup in factorisation, making it vastly more efficient.

An example of this in the real world is when, in 2019, Google claimed to have achieved ‘quantum supremacy’ with its Sycamore processor, which was able to perform a specific calculation in just 200 seconds. This same calculation would have taken the world’s most powerful supercomputer 10,000 years to complete. Google has since announced that they have begun implementing post quantum cryptography algorithm ‘Newhope’ into Chrome. This algorithm uses different methods for cryptography which have more protection against quantum computers.

Quantum Key Distribution - The Foundation for Secure Communication

Central to Quantum Cryptography is Quantum Key Distribution (QKD). Here, quantum properties enable the distribution of shared encryption keys between two parties securely. Since one of the earliest cryptographic articles published by Rivest-Shamir-Adleman in 1978, these parties have been called Alice and Bob. With QKD we bring in a third party called Eve.

With QKD, when Alice wants to send Bob a secret message, she sends a sequence of polarised photons. Quantum states used in QKD schemes like photon polarization are extremely delicate. Observing or intercepting these quantum state ‘messages’ is impossible without being discovered. Simply put, if Eve, intercepts a polarized photon, she changes its state, and this change is detectable by Alice and Bob.

This is because any act of influencing the states violates intrinsic quantum constraints like the Heisenberg Uncertainty Principle and the No-Cloning Theorem. The Uncertainty principle means measuring one property, like photon position, inherently alters another, like momentum, irreversibly, while the No-cloning principle precludes copying unknown quantum states. Together, these foundational principles ensure any interception attempts on QKD channels are detectable when Alice and Bob compare the results.

This ability to determine whether the ‘messages’ have been tampered with is far superior compared to conventional cyphers relying on RSA or other forms of encryption.

Limitations and Challenges Facing Quantum Cryptography

Despite its profound powers, practical quantum cryptography implementation must surmount several key challenges:

- Fragile Quantum States - Qubits remain prone to environmental noise and have transmission losses over long distances which can introduce errors. Here, significant hardware advances continue to improve stability and scalability.

- Trusted Infrastructure - Quantum cryptography fundamentally assumes trusted devices and communication channels. Deployment in the real world will be far more challenging.

- Range Limits - Quantum links using current fibre or satellite channels remain geographically constrained. A record link of 1200m was achieved by the Micius satellite in 2016, but longer distances would require trusted quantum repeaters which are still being developed/refined.

- Key Exchange Speed - although QKD is highly secure, it is currently much slower than the current cryptographic methods. This is because the process of generating and exchanging quantum encryption keys involves complex protocols and measurements. This is time and energy consuming.

The Road Ahead for Quantum Cryptography

Quantum cryptography unquestionably holds revolutionary potential for realizing ultra-secure communications resistant even to future quantum computers. While practical real-world quantum deployment remains nascent, the field's outlook is extremely promising. An example of this is Atom computing, which has announced a record-breaking 1225-qubit quantum computer.

Each year brings exponential advances in qubit fidelities, transmission distances, protocols, and infrastructure. Researchers are linking more and more trusted quantum partners now actively exchanging keys in limited demonstrations. Efforts from corporations like Google, governments, and standards bodies further accelerate development.

The cryptographic advantage quantum physics enables is unequivocal. As costs fall and technology matures, quantum cryptography promises to become widespread and underpin the coming quantum age's security infrastructure. Early movers staking strategic quantum positions today will reap rewards securing an expansive quantum future.

References:

Encryptionconsulting.com ‘What is RSA? How does RSA Work?’

quantumpositioned.com ‘Shor’s Algorithm: Factorising With Quantums Powerful Speedup’

Arute, F., Arya, K., Babbush, R. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5

theverge.com ‘Google is working to safeguard Chrome from quantum computers’

Spectrum.ieee.org ‘IonQ Unveils Rack-Mounted Quantum Computers’

Junyong Wang, Hongyu Chen, Zhencai Zhu. Modeling research of satellite-to-ground quantum key distribution constellations. Acta Astronautica. https://doi.org/10.1016/j.actaastro.2020.12.039

Forbes.com ‘Atom Computing Announces Record-Breaking 1,225-Qubit Quantum Computer’