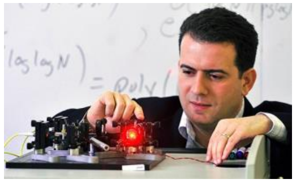
Mosca's Inequality And Its Effect On Quantum Cryptography

01/02/2019

RAM SAGAR

I have a master's degree in Robotics and I write about machine learning advancements. email:ram.sagar@analyticsindiamag.com

Intro



- Michele Mosca At the Institute for Quantum Computing
- at the University of Waterloo
- Cryptic writing is said to have come into existence as early as 1900 BC when the Egyptian scribes used hieroglyphics to communicate. The methods of cryptography might have changed over the years but the central idea hasn't changed much; either eavesdropping or evading them.
- According to Gary C Kessler, there are five primary functions of cryptography:
    1. *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
    2. *Authentication:* The process of proving one's identity.
    3. *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
    4. *Non-repudiation:* A mechanism to prove that the sender really sent this message.
    5. *Key exchange:* The method by which crypto keys are shared between sender and receiver.
- The origins of quantum cryptography can be traced to the work of Wiesner, who proposed that if single-quantum states could be stored for long periods of time they could be used as counterfeit-proof money back in 1983.
- A further advance in theoretical quantum cryptography took place in 1991 when Ekert proposed that Einstein-Podolsky-Rosen (EPR) entangled two-particle states could be used to implement a quantum cryptography protocol whose security was based on Bell's inequalities.
- The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are considered to be impossible using non-quantum communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed, keeping the eavesdroppers at bay.

Mosca’s Intervention

- In 1999, Michele Mosca played a major role in starting Waterloo’s quantum computing unit with the support of the Centre for Applied Cryptographic Research, St. Jerome’s University, and his home department, Combinatorics and Optimisation.
- Mosca’s main goal over the years has been to enable the world by building systems which are quantum-resistant and can devise encryption methodologies that will persist and be secure into a post-quantum future. Mosca provides a method for calculating that point in time – and thus came into being a basic equation – D + T ≥ Qc, that has become known as “Mosca’s inequality”
- Mosca’s Inequality equation via Ilyas Khan
- This equation states that we need to start worrying about the impact of quan n “D” (the amount of time that we wish our data to be secure for), when addec ill take for our security systems to transition from classical to post-quantum), is greater than “Qc” (the time it will take for quantum processors to have reached a scale where they can breach existing encryption protocols).

$$D + T > Qc$$

- There is now an informed consensus that at some point during 2017, Mosca’s inequality was breached and in a great many cases, D+T is significantly greater than Qc. This realisation has taken root not just at the governmental and national security levels, but increasingly within large commercial organisations.
- In one of his talks on quantum cryptography, Mosca points out that, “we are less likely to have access to timely updates on research and development in the engineering side of quantum computers from those who are building these machines. As more and more of the resource that has come into the sector is sourced from commercial organisations or ventures backed by large volumes of risk capital, competitive pressures now dictate against the publication of results in the public domain. “

Conclusion

- To explain the significance of quantum cryptography it is necessary to describe some of the important features (and perils) of cryptography in general. If QKC manages to eliminate data leaks, it also has the potential to share dangerous information without being detected by the watchdogs. So, care has to be taken in implementing prudent checks and balances in open sourcing such advancements along the way, not to forget the huge technical challenges in the form of infrastructure, that are still lurking with anything “quantum”.

END