Quantum cryptography for data heliocentric world

The heliocentrism of digital world is data and everything whirls around data. Data-driven strategy is taking center stage and has transformed the traditional technology. Data is ubiquitous and many successful businesses have realized, data is a vital asset they possess. They rely extensively on data, for designing new business model, pricing, predicting the market, competitive insights.

Today, sole existence of several global businesses is on data; for making complex decisions businesses rely on data for making meaningful intelligence. As more and more organizations are becoming data driven, securing the data is becoming the number one priority.

Recent mega-breaches have demonstrated one commonality; data is the ultimate target which attackers are behind[i,ii]. They will get there irrespective of enterprises fortified network security. As the traditional approach of network security is failing, it is wise to protect the core (data) with reinforced data layer.

Cryptography, one of the oldest domain in security, can be the most apt companion for data security. Perfectly designed cryptography with a robust algorithm and strong master key would deter attacker against all types of cryptanalysis attack.

While, cryptography is prevalent as a network layer security, but is least adopted at data layer. This is due two main challenges in cryptography key management process:

i. In multiple data breaches[iii], it was found that data was encrypted, but due to improper implementation of crucial key management process, attackers were able to decrypt into plaintext data. Key generation and distribution is an extremely intricate process to design, implement and sustain.

- Management of key exchange protocol
- Key expiry and frequent key change
- Generating unique random seed
- Complexity involved in encryption / decryption during data processing

ii. Inherent risks in traditional key generation and distribution process

- Secure storage of master key
- Risk of eavesdropping
- Susceptible to social engineering attack

These inherent initial implementation challenges and operational issues in key management process have refrained IT and application teams from adopting as data-layer security. These limitations have weakened the case for security practitioners to strongly pursue with application team for implementing data-layer cryptography.

Global technology giants and several start-ups are in a race to design and develop the fastest quantum computer, using quantum physics. As of the writing of this article, IBM had developed 50-qubit[iv] and Google announced a 72-qubit[v] system. With this speed not very far, quantum computers will be commercialized and becomes a commodity. The day this happens, attackers get access and start using the power of quantum compute and target traditional cryptography keys.

Is there an elegant solution to this present and future problem?

The answer is in quantum physics. The discovery of "uncertainty principle", in quantum mechanics, lead to innovation of "Quantum Key Distribution" (QKD) which can be the driver for exchanging secret key used in the process of encryption/decryption.

QKD can transform the way cryptography is used in data encryption and decryption.

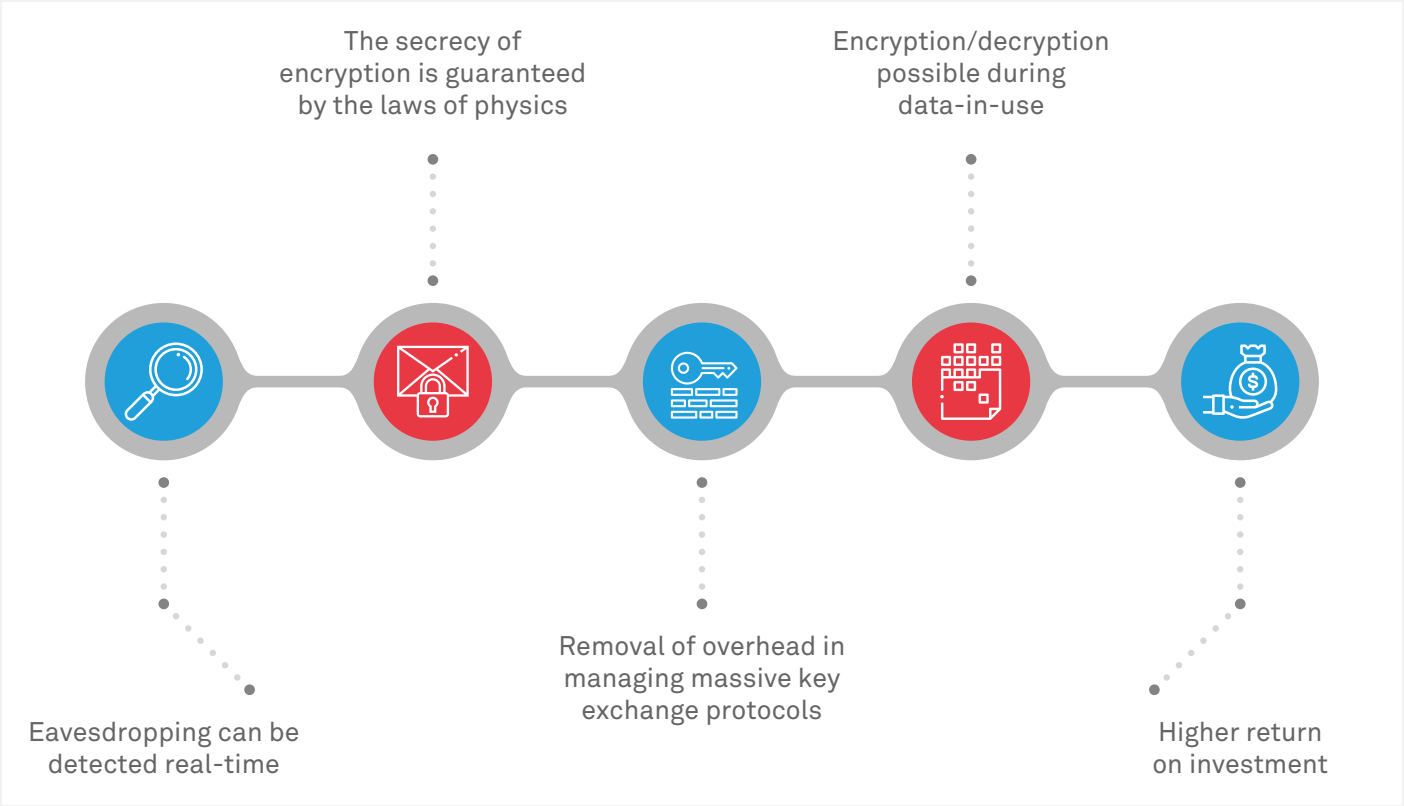

Figure: Benefits of quantum key distribution

Today commercial quantum security solution is available in the market, which is capable of secure quantum random number generator and quantum key generation and distribution. Quantum cryptography when applied to protect at the data layer, can defend data when in-rest, in-motion and in-use. Quantum random number generator (RNG) can be adopted for delivering true randomness in one-time pad encryption, the resultant ciphertext will be unyielding to cryptanalysis.

Quantum cryptography has numerous application in various business, government and industries.

Banking & finance - Core banking database

Government - Citizens unique identifier database, classified data

Defense - Voice and data communication

Critical infrastructure - Authentication records

Healthcare - Health records

IP protection - Research and development documents

The quantum technology will penetrate cloud, artificial intelligence and automation. This proliferation could have a destructive impact to traditional cryptography technologies. Enterprises opting for first-mover adoption will benefit from adequate time for planning and migration from traditional to quantum cryptography. Those who choose to wait and watch will have very less time for planning and implementation, which can lead to major business disruption. Let us proactively secure the core of digital world “Data” and leap into the quantum era.

References

[i]-https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[ii]-https://www.ftc.gov/equifax-data-breach

[iii]-http://fortune.com/2016/05/18/linkedin-data-breach-email-password/

[iv]-https://www.research.ibm.com/ibm-q/

[v]-https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

About the author

Sridhar Govardhan
General Manager and Head of Cyber Security, Wipro

Sridhar's core competency, accumulated over 18 years of professional experience, are in the business-critical domain of Cyber Defense, Information Protection and Regulatory Compliance. He spearheads organizational initiatives in building self-defensible networks, cloud security and promoting security conscious behavior in employees.

Sridhar has acquired 11 industry-recognized certifications in the domains of IT, Information Security, Security Framework and Secure Enterprise Architecture (SABSA, CISA, CISM). He holds a bachelor's degree in engineering and M. Tech from BITS Pilani; he has two patents (pending) in Cognitive Security.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/MAY 2018-APR 2019