Quantum Cryptography – A Quantum leap in Security

Jigar Kishor Thakkar[1]
Mulund, Mumbai. India
Email: jigar1859@gmail.com
*M. **+91 9819280575***

Abstract *– This paper outlines the key importance of security for all form of digital data transmission through wired or wireless channels. We begin with the volume of data being generated and the security concerns that it brings with it, making exchange of data over any channel not just "nice to have" but a "must have" layer of encapsulation. We walk through the classical idea of cryptography, the boundaries or limitations of classical cryptography and how with advent of Quantum Computers the best possible security mechanisms fail and become venerable to attacks. Further we introduce the concept of Quantum Cryptography which is derives from the principals of Quantum Physics, and how it provides a failsafe mechanism of security which cannot be compromised. To conclude we highlight some business use cases where Quantum Cryptography can be adopted.*

Keywords — *Quantum Computing, Quantum Cryptography, Classical Cryptograph, Quantum Key Distribution Algorithm (QKD, Business Impact, Quantum Cryptography Business Use Cases.*

I. INTRODUCTION

Data is being generated at a phenomenal rate. The digital Universe is growing at a staggering rate of 40% a year into the next decade, roughly doubling in size every two years. This era has also been termed as "***The Zettabyte Era***". Data is generated from large corporations (Enterprise Data), Social Media Channels, Cloud and Cloud Infrastructure, and Smart Phone or in general from Internet of Things (IoT). One of the important use of these data is of being shared amongst users, severs, devices or even multiple clouds. Movement of this data which connects cross cloud applications, requires clouds to communicate resulting in the movement of sensitive and mission critical business data. We live in the world of where Multiple Enterprises are connecting with each other to bring in collective intelligence from the user or enterprise data collected. enterprises are not just offering but embracing the cloud technologies as part of their business model thus leveraging on 3rd party and partner services. Hence, Security and Privacy are more important than ever, this paper introduces one such mechanism know as Quantum Cryptography to address this concern. Quantum Cryptography offers a failsafe solution to the problem of secure communication with unprecedented reliability

II. CLASSICAL CRYPTOGRAPHY

Classical cryptosystems as of today, use the concept of a "Key". Keys are used to encode and decode the messages that are to be transmitted over digital communication channels. There are two kinds of cryptosystems widely in place Private Key and Public Key Cryptography systems.

A. Private Key Distribution (Symmetric-key algorithm)

In a private key cryptography, two communicating parties share a single secret private key. This private key is used by the sender to encode the message and the identical shared key is used by the receiver to decode the message. As an example, let's consider Alice and Bob share a private key, known only to them, before sending the message. Alice encrypts the message using private key, Bob decrypts the message using the same private key, Alice and Bob need to find a mechanism to share the key with each other. We will later see that, this is where quantum cryptography comes in, an algorithm known as Quantum Key distribution algorithm, is the most secure method of distributing the key. Private Key Distribution is elaborated using Figure 1, indicated below.

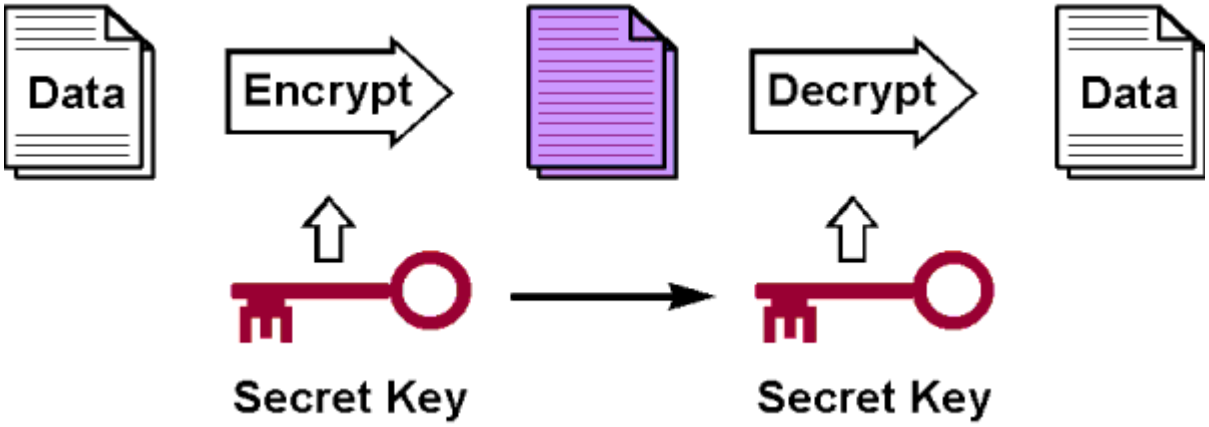

FIGURE 1 PRIVATE KEY DISTRIBUTION

B. Public Key Distribution

Public key cryptography relies on a more sophisticated approach. The receiver generates a pair of keys one public and another secret key. The public key can be shared with anyone; however, the receiver keeps the other half of the key pair all to himself, and this is his secret key. The receiver now shares the public key with the sender, who in turn uses it to encode the message. This encoded message is shared over the digital channel to the receiver. The algorithm of generation of key pairs is such that the message is encrypted using a public key, however can be decrypted only using the conjugate private key. RSA is one widely used public key cryptography algorithm. Below Figure 2 shows diagrammatically how the process works

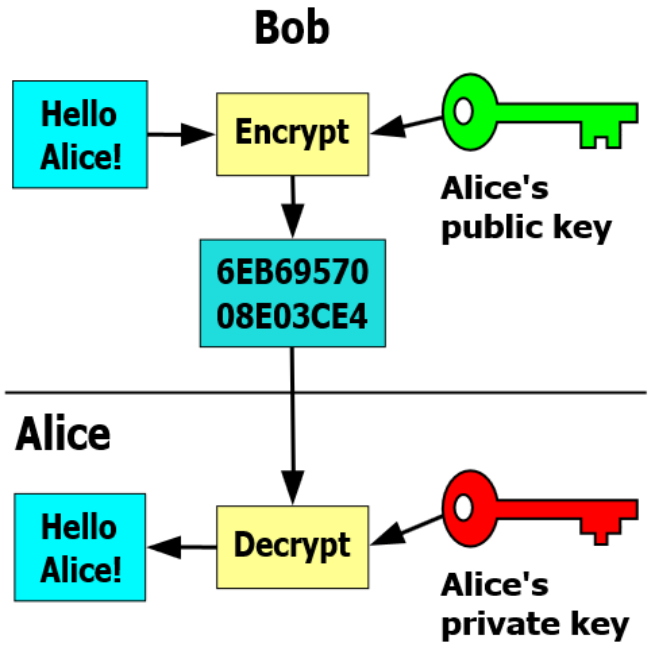

Figure 2 Public Key Distribution

Every time a product is purchased online lot of sensitive information about the user is being send over the "wire". Information such as home address, date of birth, contact information, credit card information etc. Users share this information every time they purchase a product online. Any online transaction requires the user to share most if not these personal details every time. RSA-2048 is widely used to protect the Credit card information and it is the most trusted and is very stable algorithm. However, it is not immune to the attacks, few of which include Coppersmith's Attack, Wiener's

Attack, Timing attacks, Adaptive chosen cipher text attacks, Side-channel analysis attacks, and attack against a week random number generator etc.

The largest factored RSA number is RSA-768 bits long (232 decimal digits), and the RSA-2048 may not be factorizable only until advances are made in integer factorization or computational power of classical computers soon. In theory Quantum computers provide two mechanism to break RSA one is Shor's Factoring Algorithm and using Discrete Logarithms.

III. Quantum Revolution – The Quantum Key Distribution (QKD)

Classical Cryptography systems such as RSA rely on mathematical algorithms to generate keys. These algorithms are computationally hard problem to crack although not impossible. In contrast, quantum cryptography is a method of key distribution that relies on the laws of physics quantum physics to create a key. Thus, quantum cryptography offers huge advantage over traditional methods.

Quantum Cryptography uses Quantum Key Distribution (QKD) that uses quantum mechanics. QKD uses two channels of communication one classical channel and other is quantum communication channel. The classical channel could be any ordinary classical communication link like internet, a telephone, a cell phone, a postal letter etc. Encrypted messages are sent over the classical channel, while the quantum communication channel is used to distribute quantum keys. The theory of quantum mechanics states that measurement disturbs the quantum state. Hence to learn anything about the key encoded as the quantum states, an eavesdropper must make measurements of the quantum system thus invariably disturbing the quantum system containing the keys, which is detected by both the sender and the receiver. One of the examples of a quantum key distribution algorithm is **Bennett and Brassard's protocol** published in 1984 also known as BB84. Below Figure 3 shows the QKD diagrammatically.

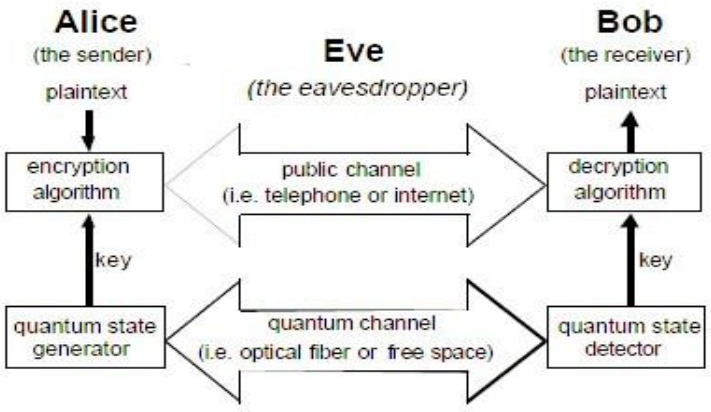

Figure 3 QKD

IV Business Impact

Big Data and Cloud, two of the trends that are defining the emerging Enterprise Computing. New paradigms in analytics such as Data Analysis as Service (DAaaS) and Internet of Everything (IoE) or boundary-less corporate networks, force companies to rethink the protection and security from the ground up. A secure key distribution algorithm such as QKD has innumerable business use cases, such secure e-commerce, m-commerce, defense communication channels, secure enterprise backup using quantum channel, Enterprise Metropolitan Area Network, High security cloud, Ultra-Secure Voting, Secure Communications with Space, A Smarter Power Grid and many more. QKD is no longer a science fantasy; QKD devices such as Toshiba QKD system are already available commercially. Nokia Inc. and Bristol University (UK) are collaborating on building an embedded optical chip on a mobile device thus bringing Quantum Cryptography to Mobile Devices The growth of quantum devices and technology opens entire new domain of applications. Which bringing robust solutions to challenges faced by businesses in handling confidential data. Often security is the key concern for businesses when using cloud services, this can be addressed very reliably using Quantum Cryptography.

V BUSINESS USE CASES

A. Quantum Cryptography to Secure Financial Transactions

Online banking is increasingly becoming more complex and sophisticated because of mobile networking. As mobile phones are becoming more popular to surf the Internet, check account balances and transfer funds between accounts worldwide, their role in Internet banking has becoming increasingly significant. As wired and wireless banking are becoming more popular worldwide, their securities continue to be major concerns among consumers. Researchers are now examining Quantum Cryptography as a possible alternative to classical encryption algorithms, such as AES, RSA. A quantum algorithm such as quantum key distribution (QKD) is the strongest candidate, whose security is guaranteed by quantum physics. Any eavesdropping will change the state of the photon that will alarm the user of the presence of hacking.

B. Ultra-Secure Voting

With political upheaval and accusations of voter fraud rampant in developed and developing countries alike, it's clear that making the voting process more secure is a necessity. Since 2007, Switzerland has been using quantum cryptography to conduct secure online voting in federal and regional elections. In Geneva, votes are encrypted at a central vote-counting station. Then the results are transmitted over a dedicated optical fiber line to a remote data storage facility. The voting results are secured via quantum cryptography, and the most vulnerable part of the data transaction (when the vote moves from counting station to central repository) is uninterruptible

C. Smarter Power Grid

It has been speculated that the American power grid is one of the most vulnerable targets for a cyber-attack. In fact, some major U.S. utilities are under "constant" attack by cyber enemies. A small encryption device called the QKarD could put an end to that fear. Using the QKarD, workers would be able to send totally secure signals using public data networks to control smart electricity grids. Smart grids are essential for balancing supply and demand for efficiency. Additionally, with proper precautions in place, they are significantly more secure than traditional grids. With the QKarD or a similar quantum encryption device, we would be able to defend and guarantee the safety of our infrastructure against attacks.

VI CONCLUSION

Quantum Cryptography is a paradigm shift in secure communications. Today's Quantum Key distribution systems provide a way to deliver secure keys on fiber optic based computer networks, which offers bit rates of 1 Megabit per second on standard telecom fiber links of length up to 100 km in length Quantum Cryptography can act as an enabler for highly secure and connected cloud. QKD can make digital commerce complete safe and reliable.

REFERENCES

[1] Quantum Computing 101
http://iqc.uwaterloo.ca/welcome/quantum-computing-101

[2] Lecture Series by Leonard Susskind, Modern Physics: The Theoretical Minimum - Quantum Mechanics by Stanford Continuing Studies Program (2012)
http://www.youtube.com/course?list=EC701CD168D02FF56F

[3] Artur Ekert, Patrick Hayden, Hitoshi Inamori, Basic concepts in quantum computation, lectures given at les Houches Summer School on "Coherent Matter Waves", July-August 1999
http://arxiv.org/pdf/quant-ph/0011013v1.pdf

[4] Image Sources:
https://dret.net/lectures/web- fall07
http://www.cse.wustl.edu/~jain/cse571- 07/ftp/quantum/

[5] Introduction to Quantum Cryptography and Secret-Key Distillation - Gilles Van Assche
http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html

[6] "The Zettabyte Era—Trends and Analysis":
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

[7] **Wikipedia References:**
https://en.wikipedia.org/wiki/Key_distribution

[8] An Overview of Cryptography - Gary C. Kessler
http://www.garykessler.net/library/crypto.html

[9] Institute for Quantum Computing
http://iqc.uwaterloo.ca/

[10] qubit.org
http://www.qubit.org/tutorials.html