Proposed Security Enhancement Conceptual Models Using Quantum Key Distribution for Future Cryptography

Phone Naing
Departmernt of Computer Science
Higher Education Centre
Pyin Oo Lwin, Myanmar
kophonenaing7@gmail.com

Kyaw Zin Oo
Departmernt of Computer Science
Higher Education Centre
Pyin Oo Lwin, Myanmar
kyawzin67@gmail.com

Mie Mie Su Thwin
Cyber Security Research Lab,
University of Computer Studies,
Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

***Abstract*— Today's Cryptographic Methods are based on Mathematical ideas and its complexity. Quantum Computers are getting increasing attention because of the tremendous power by harnessing the unique properties of Quantum Physics. When they will be able to run circles around today's computers, solving problems are infinitely faster than the world's most powerful Super Computers. So, for future Cryptographic Infrastructures, Quantum Cryptography is proposed by using Quantum Key Distribution (QKD). In this paper, it is constructed Enhancement Security Conceptual Models, QSC, Quantum Symmetric Conceptual Model and QAC, Quantum Asymmetric Conceptual Model so as to present an improvement of future cryptography by modeling being against to break Encryption Schemes from Quantum Algorithms combined with the Concepts of Mathematical and Physical Laws based on Classical Cryptography and Quantum Cryptography. Furthermore, the Security Analysis of the Performance Evaluation of the Proposed Approach is evaluated with Avalanche Effect in our Research.**

Keywords*— *Quantum Cryptography, Classical Cryptography, Quantum Key Distribution, Conceptual Model

I. INTRODUCTION

Today, secrecy, integrity, and anonymity property of our communication is achieved by Cryptography. Complex Mathematical Algorithms and Secret Keys for encryption and decryption are used by Modern Cryptography.

In our life, all classical cryptographic methods are based on mathematical assumptions of computational power, so it is unsafe when quantum computers appear because of the tremendous power by harnessing the unique properties of quantum physics. Mathematical ones rely on complexity. At the same time, it has been developing research on quantum computing based from Landauer's principle.

Either 0s or 1s are represented for classical computing and calculated by algorithm's instructions which manipulate these 0s and 1s to transform an input to an output. Qubits, simultaneously 0 and 1 are used by Quantum Computing and this property can be denoted as Quantum Superposition.

So, it has big challenge for encryption schemes because of its being based on mathematical complexity and it may be the end of encryption schemes [14]. Therefore, the scientists intensely researched on quantum key distribution via communication channels with an aim of not being able to break current encryption algorithms and defending from threat of Shor and Grover, Quantum Algorithms.

Quantum Cryptography is differed from traditional cryptographic methods in which it relies more on the laws of quantum physics rather than mathematics. Quantum key distribution (QKD) is an application of quantum cryptography which is used the principles of quantum mechanics with classical cryptography to provide unconditional security [5]. In 1984, Benette and Brassard was proposed the best known QKD protocol (BB84 protocol) and the first practical QKD experiment was carried out in 1989. The security of quantum cryptography is guaranteed by "quantum superposition", "quantum entanglement", and "Heisenberg's uncertainty principle" [13].

II. LITERATURE REVIEW

A. Conjugate Coding

Stephen Wiesner presented a class of codes made possible by restrictions on measurement related to the uncertainty principle in 1983. In this paper, it showed that in the compensation for this quantum noise and quantum mechanics allowing us novel forms of coding without analogue in communication channels adequately described by classical physics. So, he discovered several of the most important ideas in quantum cryptography on quantum information theory.

B. A New Secure Model for QKD Protocol

In 2011, the existing BB84 protocol was introduced and implemented several improvements to the basic steps in order to prevent communication partners' counterfeit, together with removing of error, gathering the information of attackers and secrecy enhancement by Rishi Dutt Sharma and Asok De. And then they compared the results of existing BB84 protocol and their proposed QKD protocol. So, they made the whole transmission process more perfect and secure from identity to the last quantum key generation and distribution so as to useful for deeper research in quantum key in the future.

C. Simulation in BB84 Protocol

In 2012, Zhu Lijuan implemented existing BB84 protocol designed with sender, .NET IDE framework and C# programming had been used for establishment and protocol simulation. And the author realized the first type of protocol simulation on the quantum simulation platform.

D. Modelling approach for performance analysis of Practical QKD Protocol

In 2015, Minal Lopes and Dr. Nisha Sarwade discussed the approach of simulation to understand and test the

working of practical prepare and measure QKD protocol. The authors experimented test-data of three QKD setups in their model. Then they analyzed quantum bit error rate and secret key rate for performance parameters and it was detected that the experimental results matched with simulated results.

E. Improvement of QKD Protocol

In 2020, Zisu Liliana attended in "Ferdinand" Military Technical Academy, Romania, presented an improvement of the protocol by using quantum memory and coding two, three or four bits for each photon. It got the efficiency of protocol, depending on the number of encoded photons.

F. Inspired to construct our proposed conceptual model

Quantum computers are getting increasing attention because of the tremendous power by harnessing the unique properties of quantum physics. When they will be able to run circles around today's computers, solving problems are infinitely faster than the world's most powerful supercomputers. It is very useful for financial services (banks, credit unions, savings institutions, and credit card companies, etc.), and businesses where required secure data communications. Simultaneously, the development of quantum cryptography is increased astonishingly.

Unfortunately, involving for the above research papers, there has no research on adequate standard models combined with classical and quantum cryptography, recently, to defend the threats of quantum algorithms in every research center and research university all over the world even in CERN (The European Organization for Nuclear Research).

III. PROPOSED CONCEPTUAL MODEL

The core objective of this research is to develop for the near future of Cryptography. The proposed Security Enhancement Conceptual Model is constructed as in the assumptions of Quantum Physics and Mathematical Computation Power that based on complexity. The proposed Conceptual Model incorporates two parts; Quantum Key Distribution that involves in the Laws of Quantum Physics, and Classical Cryptographic Methods that involve in the complexity of mathematical computations.

A. Classical Cryptograhic Methods

Classical cryptography has two mainly cryptographic algorithms which are symmetric and asymmetric algorithms.

Symmetric cryptographic algorithms use only one secret key for encryption and decryption electronic information. There are two types of symmetric cryptographic algorithms such as block and stream algorithms. The block algorithms in which the lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key and the data is being encrypted, the system holds the data in its memory as it waits for complete blocks. The stream algorithms in which data is encrypted as it streams instead of being retained in the system's memory.

Some popular symmetric cryptographic algorithms are - DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), RC4 (Rivest Cipher 4), Blowfish (Drop-in replacement for DES or IDEA), etc.

Asymmetric Cryptographic Algorithm is a part of cryptography where a secret key can be divided into two parts, a private and public keys. The public key can be given to anyone, trusted or not, while the private key must be kept secret. Some examples of asymmetric algorithm are X25519 key exchange, Ed448 signing, X448 key exchange, RSA, Diffie-Hellman key exchange, DSA and etc. Among them, RSA encryption algorithm is one of the most powerful forms of encryption in the world. It supports incredibly key lengths, and it is typical to see 2048- and 4096- bit keys.

B. Quantum Key Distribution(QKD)

For Cryptographic Protocols, Quantum Key is used for distributing secret keys. Ensuring that they remain private is the crucial one. On single photons, information is encoded typically shown in Fig 1.

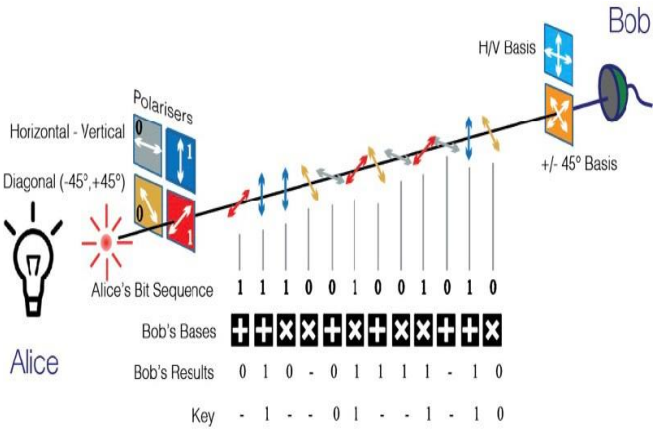

Fig. 1. Vertical (V) or Horizontal (H) polarisation of QKD

Alice can choose to encode these in a "bit sequence" using one of two states, like vertical (V) or horizontal (H) polarization, and she also can chose to encode in two different states; here, two combinations of these states labeled +45° and -45°. Bob then choses to measure in one of the two, also known as bases – either he measures H,V, or he measures +45°, -45°. If he measures in a base that is different from the one Alice used to prepare, then his answer will be random and discarded, but if they chose the same one, then they will have perfectly correlated results; Alice sends H and Bob detects H, and these are kept [15]. This last step requires Alice and Bob to communicate about which base was used but reveals no information about the result, which now becomes the secret key. This is just one way to do but there are now many variations.

It is just generated a secret key, then needed to be incorporated into cryptographic protocols to ensure security in the various applications. BB84 was originally described using photon polarization states and quantum entanglement was required. BB84 protocol requires measurement in two different orthogonal bases. The beauty that quantum physics brings to this solution is that if a spy or a hacker tries to intercept the key generation, they will introduce errors and reveal themselves. Importantly, this happens before any information is encoded or communicated[8,9].

C. Proposed Quantum-Symmetric Conceptual Model

In our proposed Quantum-Symmetric Conceptual Model, it is used for both Block Cipher Algorithm and Stream Cipher Algorithm. For initial key distribution, it is introduced in Quantum Key Distribution. In Fig 2, it shows our Proposed Quantum-Symmetric Conceptual Model.

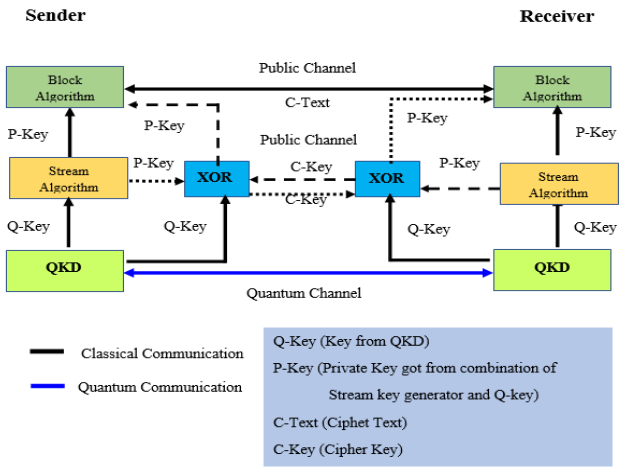

Fig. 2. Proposed QSC, Quantum-Symmetric Conceptual Model

In every Symmetric Algorithm, there has been only attacked by Statistical Methods. Firstly, attackers compute frequency of each letter in Cipher Text. And then they make assumptions about the distribution of letters, pairs of letters examining Cipher Text and correlating properties with the assumptions. So, in proposed model, it is used Stream Cipher Algorithm for the keys and Block Cipher Algorithm for the Cipher Text.

Being Advanced Secure Symmetric Algorithms, it is needed to completely obscure statistical properties of original message. Therefore, it is used confusion method and diffusion method. Diffusion method dissipates statistical structure of plaintext over bulk of Cipher Text. For example, if we change a single bit of the plaintext, then half of the bits in the Cipher Text should change and in the same way, if we change one bit of the Cipher Text, then approximately one half of the plaintext bits should change. Confusion method makes relationship between Cipher Text and Key as complex as possible to prevent the attackers from deducing the key. So, each binary digit of the Cipher Text should depend on several parts of the key, obscuring the connection between them.

Stream Cipher Algorithm is very fast as only used in diffusion method. Therefore, it is used to combine QKD key and session key in order to get private key for using in block algorithm. Block Cipher Algorithm uses more time consumption than stream cipher because of using both diffusion and confusion methods. With the aim of enhancing in security of the Cipher Text, it is used for Encrypting Text. Moreover, even in the use of Private Key got from QKD key and Stream Session Key, it is again XORed with QKD key to get Cipher Key.

This proposed QSC system consists of mainly two parts, sending site and receiving site. AES, RC4 algorithms are used for encryption and decryption processes. RC4 is used for encryption of session key got from key generator combined with XOR operation. AES is used for encryption and decryption of plaintext. It is implemented a privacy good quantum cryptographic system, enhancing original BB84 protocol, and combining symmetric algorithms. Now it is implemented with Colored Petri Nets (CPN) Tools which is used for editing, simulating, and analyzing high-level Petri nets and having a simulator and including a state space analysis tool as shown in Fig.3.

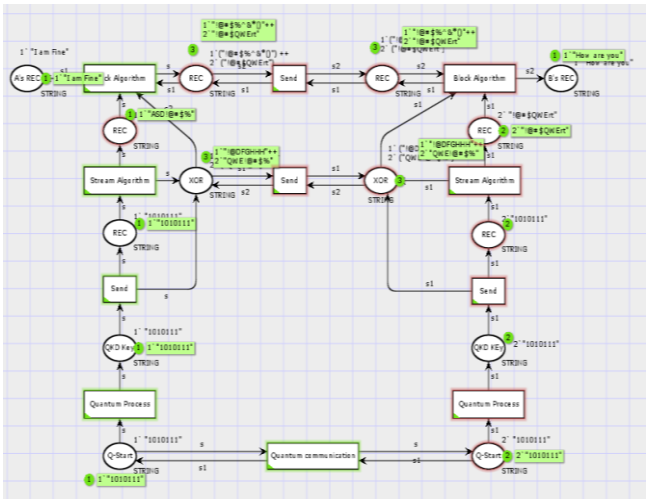

Fig. 3. Petri Nets Model of Proposed QSC, Quantum-Symmetric Conceptual Model

D. Proposed Quantum-Asymmetric Comceptual Model

In our proposed Quantum-Asymmetric Conceptual Model, the initial key distribution is introduced in Quantum Key Distribution. This proposed model is illustrated in Fig 4.

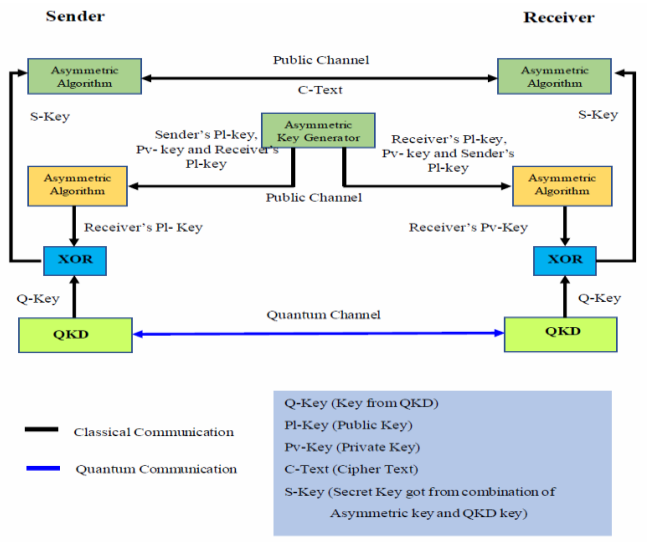

Fig. 4. Proposed QAC, Quantum-Asymmetric Conceptual model

In every Asymmetric Algorithm, there has been mostly attacked by Mathematical Attacks. It is analyzed by the underlying in complexity of Mathematical Factoring Theorem. RSA cryptosystem which is broadly used for secure data transmission in the Internet and it derives from the fact that the factoring problem is “hard.”

However, in 1994, Peter Shor showed that a quantum computer could be used to factor a number n in polynomial time, thus effectively breaking RSA. The efficiency of Shor's Algorithm is due to the efficiency of the Quantum Fourier Transform, and Modular Exponentiation by repeated squaring. If a Quantum Computer with a sufficient number of Qubits could operate without succumbing to quantum noise and other Quantum-de-coherence Phenomena, then

Shor's algorithm could be used to break public-key cryptography schemes. For the fact that we combined Public Key and Private Key with QKD by XORing to get Q-Public Key and Q-Private Key as soon as they had shared pair of keys with an aim of preventing and defending from Shor's Quantum Algorithm.

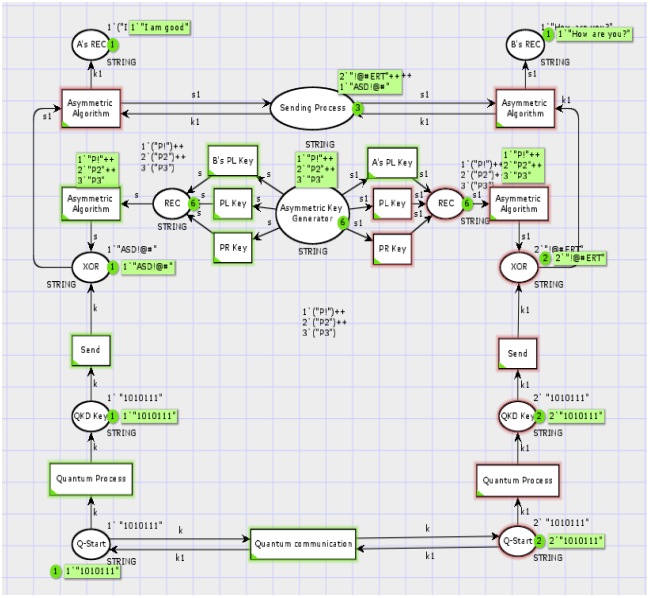

Fig. 5. Petri Nets Model of Proposed QAC, Quantum-Asymmetric Conceptual Model

This proposed system consists of mainly three parts, sending site, receiving site and key generation server. RSA algorithm is used for encryption and decryption processes. It is implemented a privacy good quantum cryptographic system, enhancing original BB84 protocol, and combining asymmetric algorithms. Now it is implemented on the modelling of QAC System with Petri Nets Tools as shown in Fig 5.

Two Security Enhancement Conceptual Models, , QSC, Quantum Symmetric Conceptual Model and QAC, Quantum Symmetric Conceptual Model Using Quantum Key Distribution for Future Cryptography have been proposed.

IV. Performance Evaluation using Avalanche Effect

Avalanche effect is concerned with a specific behavior of mathematical functions used for encryption in Cryptography. It is considered as one of the desirable properties of any encryption algorithm. Either the key or the plaintext has a slight change, the change in the cipher-text should be produced significantly. This property is identified as avalanche effect. Avalanche effect was analyzed on this encryption technique. A change in one bit of the plaintext or key should produce a change in many bits of the ciphertext can be defined as Avalanche effect. Simply, it quantifies the effect on the ciphertext with respect to the small change made in the key or plaintext.

Shannon's property of confusion and diffusion identified the concept of avalanche effect. However, the term was first stated by Horst Feistel. It should be considered as one of the primary design objectives in implementing a strong cipher or cryptographic hash function, this should be considered as one of the primary design objectives.

A slight change in an input data of the algorithm that uses hash value should change apparently.

The algorithm that applies hash value, even a slight change in an input data should apparently change the value of hash. Similarly, flipping single bit in input data should at least flip half of the bits in the hash value.

If the encryption algorithm satisfies the relationship below, we can say that it is a good encryption algorithm.

"Avalanche effect is greater than 50 Percentage"

It can ensure that a plain-text through a statistical analysis cannot be easily predicted by any attacker. If the encryption algorithm cannot satisfy this property, we can say that it is not a secure algorithm.

Avalanche Effect can be computed by using the following equation.

Avalanche effect=(Hamming distance/Block size)*100%

By calculating the above formula, the percentage of the data changed will be resulted. If the result change more, the system will secure more.

The performance evaluation of the comparative security analysis between (AES-256+BB84) and QSC and RSA and QAC using Avalanche Effects are discussed below. The following tables show Avalanche Effect due to 1-bit variation in plaintext keeping the key constant and Avalanche Effect due to 1-bit variation in key keeping the plaintext constant between (AES-256+BB84) and QSC, as well as between RSA-1024 and QAC.

A. Security Analysis Between (AES-256+BB84) and QSC

In (AES-256+BB84), it is used Plain Text Block of 128-bit and key bits 256. For the security, it is measured one bit of the plain text or the key is changed, it produces several bits of the cipher texts changed and it is also defined as the Avalanche effects of its algorithm. Table I and Table II are shown these effects on (AES-256+BB84) bits algorithm.

TABLE I. Avalanche Effects of (AES-256+BB84) on Plaintext without Mapping in Binary Codes

Plain text variation of 1-bit with constant Key	Avalanche Effects (%)
60	46.67
68	53.15
53	41.40

TABLE II. Avalanche Effects of (AES-256+BB84) on Key without Mapping in Binary Codes

Key variation of 1-bit with constant plaintext	Avalanche Effects (%)
68	53.13
63	49.21
66	51.56

In our proposed QSC model, it is used not only stream algorithm for the key combined with QKD keys but also block algorithm for encrypting plaintext. It is implemented the Avalanche effects as shown in Table III and Table IV.

TABLE III. AVALANCHE EFFECTS OF QSC MODEL ON PLAINTEXT WITHOUT MAPPING IN BINARY CODES

Plain text variation of 1-bit with constant Private Key	Avalanche Effects (%)
72	56.25
71	55.47
70	54.67

TABLE IV. AVALANCHE EFFECTS OF QSC MODEL ON PRIVATE KEY WITHOUT MAPPING IN BINARY CODES

Private Key variation of 1-bit with constant plaintext	Avalanche Effects (%)
93	72.66
120	93.75
116	90.62

B. *Security Analysis Between RSA and QAC*

RSA algorithm supports 2048 key lengths, and 4096-bit keys. For the Avalanche effects on the testing of security, it is implemented on the Table V and Table VI in 2048 bits.

TABLE V. AVALANCHE EFFECTS OF RSA ON PLAINTEXT WITHOUT MAPPING IN BINARY CODES

Plain text variation of 1-bit with constant Public Key	Avalanche Effects (%)
55	44.55
60	48.95
65	52.12

TABLE VI. AVALANCHE EFFECTS OF RSA ON PUBLIC KEY WITHOUT MAPPING IN BINARY CODES

Public Key variation of 1-bit with constant Plaintext	Avalanche Effects (%)
72	50.12
70	49.22
81	53.65

In our proposed QAC model, it is used RSA 2048-bits algorithm combined with QKD keys so as to defend quantum algorithms like Shor's algorithm. It is implemented the Avalanche effects as shown in the following Table VII and VIII.

TABLE VII. AVALANCHE EFFECTS OF QAC MODEL ON PLAINTEXT WITHOUT MAPPING IN BINARY CODES

Plain Text variation of 1-bit with constant Secret key	Avalanche Effects (%)
77	54.55
79	55.95
76	53.32

TABLE VIII. AVALANCHE EFFECTS OF QAC MODEL ON SECRET KEY WITHOUT MAPPING IN BINARY CODES

Secret Key variation of 1-bit with constant Plain Text	Avalanche Effects (%)
93	73.66
112	91.96
120	93.61

C. *Comparative Study of the Performance Evaluation Summary*

The performance evaluation summary of the comparative security analysis between (AES-256+BB84) and QSC using Avalanche Effects is as shown in Figure 6. It is so obvious to see that our Proposed QSC is more secure than the (AES-256+BB84).

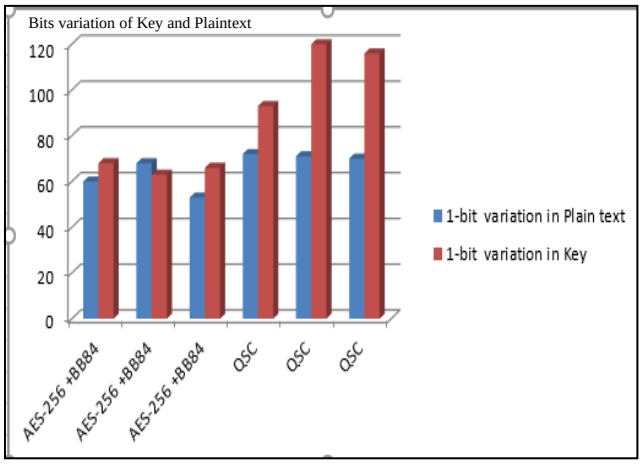

Fig. 6. Comparative Study of the (AES-256+BB84) and QSC using Avalanche Effects

The performance evaluation summary of the comparative security analysis between RSA and QAC using Avalanche Effects is as shown in Figure 7. It is so obvious to see that our Proposed QAC is more secure than RSA.

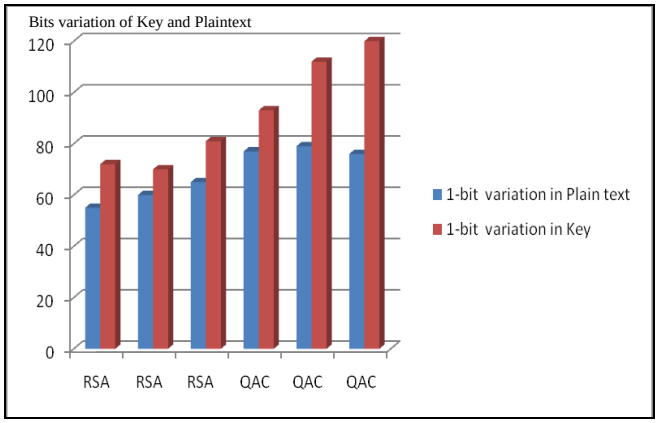

Fig. 7. Comparative Study of the RSA and QAC using Avalanche Effects

V. CONTRIBUTIONS OF THE PROPOSED APPROACH

- Enhancement Security Conceptual Models, QSC, Quantum Symmetric Conceptual Model and QAC, Quantum Asymmetric Conceptual Model are modeled by the ccombined cconcepts of Mathematical and Physical Laws based on Classical Cryptography and Quantum Cryptography are proposed.
- In this paper, we can also prove by using Avalanche Effects that our Proposed QAC and QSC are better than the (AES-256+BB84) and RSA.
- Shared Key cannot be determined alone, so both parties influence the outcome of the protocol.

- Information can be shared securely with others including groups of users and company departments.
- It provides unconditional security as the key is random and authenticated .
- Eavesdroppers do not have sufficient information to determine the plaintext because there is no relationship between cipher-text and plain text.

VI. FINDINGS

Due to the evolvement of Quantum Computing and Quantum Computers, Classical Cryptographic Systems will not be able to guarantee for total security.

Conventional Crypto Systems use one key, or Asymmetric encryption, which uses two that is based on mathematics. But in our research system, it has implemented two keys that are got so different from mathematics and quantum physics.

But Quantum Channel can only work over a limited distance.

VII. CONCLUSION

Being fast development of Science and Technologies, the information security becomes critical in our daily life. This paper objectively aims at constructing proposed Conceptual Models for development of future Cryptography. It has implemented a better privacy cryptographic system using QKD keys being based on symmetric algorithms and asymmetric algorithm.

After the involving of Quantum Computer, the security of Classical Cryptography using in today would has been threaten. Surely, we can point out that if we could develop and apply QKD in current world, all the hackers and code breakers will simply become unemployed. Continuously, in very near future, 5G Network age, QKD protocol can be expanded very gratefully in electronically transferred and process systems.

REFERENCES

[1] A. Muller, J. Breguet, and N. Gisin,"Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km," Europhysics Lett. 23, 383–388 (1993).

[2] C. Marand and P. Townsend, "Quantum key distribution over distances as long as 30 km," Opt. Lett., 20, 1695–1697 (1995).

[3] C. Shannon, "Communication theory of secrecy systems," Bell System Technical J. 28, 656–715 (1949).

[4] "History of cryptography," article in Wikipedia (retrieved on 2019-9-11), http://en.wikipedia.org/w/index.php?title=History_of_cryptography&oldid=83652220

[5] Hughes, Richard J., D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, Quantum cryptography, Contemporary Physics, Vol. 36, No. 3(1995).

[6] J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits," J. Mod. Opt. 41, 2405– 2412 (1994).

[7] Justin Winkler, "Entanglement and Quantum Key Distribution," http://www.optics.rochester.edu/workgroups/lukishova/QuantumOpticsLab/2010/OPT253_reports/Justin_Essay.pdf

[8] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature 414, 883–887 (2001).

[9] Pankaj, "Difference between Classical and Quantum Cryptography," https://www.geeksforgeeks.org/differences-between-classical-and-quantum-cryptography/

[10] Rifaat Zaidan Khalaf, "Quantum Encryption Algorithm Based on Modified BB84 and Authentication DH Algorithm," Thesis for Doctor of Philosophy in Applied Mathematics and Computer Science, 2015, Eastern Mediterranean University.

[11] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM 21, 120–126 (1978).

[12] S. Singh, The Code Book (Fourth Estate, London, 2000).

[13] Vadim Makarov "Quantum cryptography and quantum cryptanalysis," Norwegian University of Science and Technology

[14] W. Stallings, Cryptography and network security: principles and practice (Prentice Hall, 3rd edition, 2003).

[15] https://qt.eu/discover-quantum/underlying-principles/quantum-key distribution-qkd/