ANALYSIS OF QUANTUM KEY DISTRIBUTION IN CRYPTOGRAPHY AND ITS APPLICATIONS

Dr. Ambika R[1*], Dr. Anilkumar D[2], Shashikala J[2]

1,2 BMS Institute of Technology and Management, Bengaluru, India

(Email id:ambikr@bmsit.in, anilkumard81@bmsit.in, shashikala_j@bmsit.in)

(Corresponding author: Dr. Ambika R: Email id: ambikar@bmsit.in)

Abstract: Safe communication is a growing concern in almost every sector. The data was encrypted using cryptographic techniques. Compared to traditional cryptography, quantum cryptography is a strong and optimistic step. Our data would be safer than in the past if quantum encryption is used in the right way. To protect the confidential information to be transmitted, cryptographers are trying to develop more sophisticated techniques. But hackers, code breakers and eavesdroppers are working furiously to break the systems. As security is achieved by either cryptographers or security is breached. The success is, however, provisional. The method of protecting the message using a deciphering device and of breaking the system. In this article, various quantum encryption and distribution methods are discussed and analyzed.

Keywords: **Classical Cryptography, Quantum Cryptography, Quantum Key Distribution, Avalanche Effect**

1. INTRODUCTION

Protecting significant and important data is of utmost concern to the organization or multiple input, multiple output transmitter-receiver-based communication system. Cryptography is one of the key techniques of protecting the data. Novel concept in cryptographic security is the Quantum Encryption. Quantum cryptography uses quantum fluctuations of laser light at the physical layer which is introduced into the existing network. This enables extreme-secure communication and perfect security. Security is an important characteristic of any network with special reference to mobile - adhoc networks. The wireless networks are potential for hacking using mobile devices. There is no clear line of defence for protecting any mobile network. Development of mobile application security system, which uses a layered security approach and strong cryptographic techniques is the probable and low-cost solution to protect such application-based wireless networks.

Quantum key distribution is a cryptographic protocol and it allows two communicating parties to distribute a secret key in the presence of an eavesdropper [1]. Quantum cryptography uses quantum mechanical concepts such as the Heisenberg uncertainty principle and the no-cloning theorem in order to ensure that Eves dropper cannot gain non-negligible amount of information without **being detected, even if his/her computational power is** unlimited. This paper discusses about the review of the work carried out using quantum cryptography and defines various terms related to it.

2. LITERATURE REVIEW

In this section, related articles on key generation, distribution and quantum key distribution have been reviewed and analyzed.

Ambika R. et. al., introduced a data protection multi-transceiver system [2]. They considered three users and implemented RSA commutative and proved RSA algorithm's commutative nature. In this paper, authentication is accomplished by key exchange approach and the limitation of the same is discussed. In most of the existing data authentication or security systems, overhead of key exchange has been increased. To achieve the goal of data security with individual encryption/decryption without affecting the data security and its integrity, a modified RSA has been developed and this mechanism is known as Commutative RSA. The device communicated is secureand can not be colluded . In general, the use of cryptographic techniques is favored, hence the proposed Multi FPGA core protocol in this paper adopts the commutative RSA algorithm.

In this paper, a security or authentication was implemented for multiple MIMO or transceiver terminals using the public key cryptography technique called Commutative RSA. The goal of data security is implemented in multiuser communication environment. The commutative RSA approach has been implemented with multiple FPGA cores that function as an individual transceiver terminal and perform its individual encryption without affecti ng the original data. Serial Montgomery multiplication was planned and simulated with multiplier with multiplier Radix-2. The results achieved have been compared, and the new Serial Montgomery architecture has been found to work better than previous architectures.

In this paper, the commutative RSA core was implemented for simulation and illustration of data authenticity among multiple user terminals in a communication environment on multi ple FPGA devices.

Normand J. Beaudry et al., demonstrated a general method for proving the security of quantum key distribution protocols in two ways [3]. First is based on super dense coding, and second is based on the LM05 dual-way protocol. They proved that an eavesdropper secures these two protocols against other, more common forms of attacks.

Highly robust and optimized system architecture has been proposed for implementing a commutative RSA algorithm for data authentication among multiple MIMO terminals, simulated on FPGA devices in [4]. A noble commutative RSA approach has been implemented to facilitate secure data communication among multiple input multiple output channels or transceiver systems. Commutative RSA states the order in which encryption is performed does not affect the encryption output.

Authors implemented and simulated the complete code on several FPGA devices. The robust Montgomery modular multiplication mechanism has been adopted with radix-2 multiplication architecture to maximize device output with limited space and higher speed. Authors have proposed the implementation of the CRSA cryptography core based on serial Montgomery and parallel Montgomery with the aim of improving device efficiency for its lower memory occupancy, rapid pace, higher throughput and lower power consumption.

Conventional cryptosystems such as ENIGMA, Data Encryption Standard or even RSA are based on a mixture of mathematics and guesswork [5]. In formation theory has shown that traditional secret-key cryptosystems can not be completely secure unless the key, which is only used once is at least as long as the cleartext.

On the other hand, the principle of computational complexity is not well established to pr ove
the computational security of public-key cryptosystems. The writers in this paper use a radically different cryptographic base. They used a quantitative physics uncertainty theory.
Through modern information theory and cryptography, digital messages can often be passively tracked or copied through practice, even by someone ignorant of what they say. However, when in non-orthogonal quantum states information is encoded, for instance single photons with polarization directions 0, 45, 90 and 135 degrees, a communication channel is obtained whose transmission cannot, as a rule, be copied, read or copied reliably by an eavesdropper who is ignorant of such essential information used to render transmission. Without altering a random, uncontrolled manner that could be detected by the legitimate users of the chann el,
the cryptanalyst or attacker can not obtain partial information about such a transmission either.
Information security is important in today's world and in future for data confidentiality sin ce
we expect our digital opponents to be fingerprinted with more powerful computers and ne w
algorithms. The advent of quantum computers that are capable of launching effective attac ks on conventional techniques, such as the commonly used types of public key cryptograp hy, is of particular concern [6].

Since the protection of quantium cryptography relies solely on the local
Equipment of the legitimate users, the key challenge in the implementation of quantum cr yptography is to determine how much information these equipment leaks to possible oppo nents. If this information leakage can be restricted under a certain standard, a security tech nique called the data protection extension can be used to recover it. This compresses a par tly secret bit-
sequence to a highly secure key and depends on the estimated information leakage, the co mpression. Thus, the security promise of the theoretical protocol against available technol ogies can be restored by properly characterizing a true framework.

Data protection enhancement is not the only resources available to ensure the safety of quantum cryptography implemented. Hardware and protocol modifications can dramatically reduce the lack of information and the potential for lateral channels and active attacks. In addition, thehardware of a real system can be tested with quantum correlations. These tests may be demanding to perform but have the advantage of immunity from a wide range of problems with implementation [7].

Makhamisa Senekane et. al, suggested the six-stage quantum key distribution protocol to implement its optical implementation [8]. This protocol uses more detector range and improves its consistency, increases the likelihood of discrimination, and improves detector.

Mohd Asad Siddiqui, Tabish Qureshi have proposed Quantum Key Distribution method. In this, user A sends user B pairs of qubits and each is in one of four states. User B genera tes a secure key with one qubit and a subsidiary key with the other. He randomly determin es for what pair which key to use. In order to match the safe key of user A, an auxiliary ke y must be added to the safe key of user B. This scheme gives the BB84 standard protocol an additional security layer [9]. Between two remote parts, a secret key is generated, and a quantum channel is used. The hidden key may be used Vernam Cipher or single pads to send encrypted messages.

Cipher Vernam is very secure given that a key is exchanged. Secure messaging applications are based Android and Web-based systems that are used to securely send messages among registered users to any company using cryptographic algorithms [10]. U ntil sending the message the application can be protected by user authentication. The safe messaging system uses minimal overhead processing while maintaining safety. Authentication of each user is strengthened using Salt in the database to store sensitive credentials for each user. Message encryption and decryption was done using the Advanced Encryption Standard monoalphabetic algorithm.
This algorithm is actually less secure than the key- public encryption method.
This is the principal restriction of this work.
An eavesdropper breaking in into the message returns an insignificant message. encryptio n and decryption are clearly one of the easiest ways to conceal the meaning of a message from interferers in a network environment.

3. IMPERFECT ENCODING

That Quantum Key Distribution Protocol needs to determine how the quantum states to be sent over the unstable public channel are to be prepared. This is analogous to the initial selection of good prime numbers in the RSA algorithm, where a poor selection can jeopardize overall protection.

The prepared countries may differ from those specified
in the protocol for the purposes of Quantum Key Distribution due to physical equipment imperfections. This suggests that the impact on security should be small.

However, the outcome does not standardize the usual losses of a communications channel when standard security tests are implemented, which results in a much higher rate of lowering than expected.
This condition has been overcome by recent safety proof, which is available in the finite-size case as well as asymptotically endless key blocks.
These proofs can be used to calculate the difference between the ideal model and to restore the protection of a Quantum Key Distribution system and achieve almost the same key generation rate as for faultless encoding.

4. PHASE CORRELATION BETWEEN SIGNAL PULSES

In multi-photon emissions, a replacement of the ideal sngle-photon light sources with reduced laser is common in the Quantum key distribution. One of the consequences of this substitution is that the electromagnetic phase of each light pulse emitted may partly be linked to the other pulse phase because of its las er consistency. Therefore, it is very necessary to have phase correlation in quantum key cr yptography between signal or quantum codes.

A. Bright-light attack

The single photon detectors are key components of most Quantum Key Distribution syste ms. The weak optical signal received by the transmitter via a communications channel is detected in the Quantum Key Distributor receiver. Lawrence photodiodes that work in Geiger mode

are the most common detectors for single photons.
The Avalanche Photo Diode is biased over the decompose voltage to make a single photon easily detectable through sudden growth in the output current by triggering a self-sustaining avalanche.
However, any detector needs to spend some of its time under a collapsing voltage, becaus e at some point the detection avalanche needs to be shut down to reset the detector. The detector enters the linear mode when it is no longer sensitive to single photon radiation.

It has been demonstrated that Eve can use the linear regime to monitor the detector output deciding bits of the final key unnoticed. Even can also force a single photon detector into t he linear mode in some situations, send a bright light into the receiver module and take ad vantage of its control abilities and steal key bits.

It is important to analyze this group of attacks carefully and make efforts to distinguish between the incorrect running of a detector and real loopholes. For example, when handling gated Avalanche Photo diodes in a specific mode, bright illumination from a continuous-wave laser of 1FW – 10mW was easily detected. The APD parameters such as photo current, bias tension, temperature, after-pulsing rate or quantum efficiency can be also monitored on an on-line Quantum Key Distribution system.

These countermeasures dramatically reduce information Eve is able
to obtain from the key, and current research continues to calculate its effect precisely on the safe key rate.

B. Efficiency mismatch and time-shift attacks

The Quantum Key distribution configuration consists of two detectors, which are correlat ed with either 0 or 1. If an adversary is able to figure out which of the detectors answered the input light, he will learn the key bit. It is therefore necessary to distinguish two detecto rs from the point of view of the opponent. This is challenging because it is impossible that 2complex objects such as photo detectors would be the same. general the opponent has o ptions to attack the Quantum Key Distribution configuration if the response curves of the devices are different.
In addition, if the detector efficiencies vary in wavelength, an opponent can attempt to attack "efficiency-match," while an opponent may launch the "time-shift" attack if the time responses are different.
Another attack was recently described to deliberately induce a detector malfunction.

The combination of PA and the differences in the parameters of the two detectors can be used to prevent this kind of attack. The safety evidence considers the difference between detector response curves and removes the additional information leaked through PA to an opponent.
The symmetrisation of the detectors with regard to a single photon signal condition can al so deny this attack. The two detectors will be virtually identical by randomly switching th e bit allocation between the two detectors, thereby preventing one opponent from assignin g bit values to the information it gets.

C. Back-flash attack

The backflash attack is a passive way to let an opponent learn the bit values associated wit h detection events. During the avalanche of charging carrers due to a detection event, the s econdary photons emitted byan Avalanche PhotoDiode that travel back to an opponent fro m the detectors through the transmitter communication canal.This effect was demonstrate

d in gated detectors InGaAs / InP routinely used in QK systems with a wavelength of tele communications.

The backflash attack is a passive way to let an opponent learn the bit values associated wit h detection events. During the avalanche of charging carrers due to a detection event, the s econdary photons emitted by an Avalanche PhotoDiode that travel back to an opponent fr om the detectors through the transmitter communication canal.This effect was demonstrat ed in gated detectors InGaAs / InP routinely used in QK systems with a wavelength of tel ecommunications.

In order to prevent a back-flash attack, proper design and analysis of Quantum Key distribution systems can be carried out. Some solutions may involve low-loss passive optical devices such as insulators, circulators, or special filters, which link the likelihood of a photon leaking back from the quantum key distribution system to a low level in order to recover security using passive attack. The use of a short gate will also reduce the light emission intensity in fast-moving detectors significantly.

5. CONCLUSION

Intense and prolific research over the past twenty years has been triggered by quantum cry potgraphy and Quantum Key Distribution. Quantum Key Distribution allows secret key cr eation by means of a combination of a conventional channel and a quantum channel, s uch as an optical fibre connection or an optical open- space linking.
Quantum Key Distribution's primary value is that all eavesdropping can be observed in th e rows, connected intrinsically to the "quantum" of the transmitted signals in the quantum channel.

This property gives rise to a cryptographic property that can not be obtained by classical techniques, which enables the Key Establishment to operate under an extremely high security standard, called unconditional security or theoretical information security. The natural candidates for Quantum Key Distribution based security solutions are therefore highly security applications.
However, many important issues remain to be solved. A further prospect is to examine and demonstrate the integration of quantum key distribution into real security infrastructures alongside the existing challenges related to theory and experimentation of Quantum Key distribution.

In order to take full advantage of the opportunities provided by point-to - point distance-restricted quantum key distribution links, it is important to develop a network architectures. However, the Quantum Key Communication Networks are not all-round networks they are locked, hidden and distant, and their characteristics are closely related to their physical layer's quantum characteristics.
Such networks therefore differentiate essentially from the conventional Key Distribution infrastructure. We nevertheless find the use of Quantum Key Delivery networks in high-security
environments which until now relies solely on trustworthy couriers from Key Establishme nt to be promising.In the context of safe networks based in symmetric-key encryption systems, Quantum Key Distribution-based systems can also be regarded as an alternative to public-Key session key exchange.
In conclusion, the Quantum Key Distribution Network is a security network that enables the theoretical distribution of key information over a worldwide network.
We hope their evolution can be combined successfully with "classical cryptography"

ideas that
open promising paths towards progress in cryptography and safety in the networks.

FUTURE SCOPE

In this paper we have analysed various quantum key distribution techniques along with classical key distribution. Our work will continue in enhancing some of the techniques using GPGA for better efficiency and throughput.

REFERENCES

[1] *N. Sasirekha, M.Hemalatha (2014), Quantum Cryptography using Quantum Key Distribution and its Applications, International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-3, Issue-4.*

[2] *Ambika R et.al., "Data Security Using Serial Commutative RSA Core For Multiple FPGA System"(2014), Second International Conference on Devices, Circuits and Systems, DOI: 10.1109/ICDCSyst.2014.6926198*

[3] *Normand J. Beaudry et. Al., "Security of two-way quantum key distribution" (2013), American Physical Society, A 88, 062302.*

[4] *Ambika R et.al., "Securing Distributed FPGA System Using Commutative RSA Core" (2013), Global Journal of Researches in Engineering, Vol 13, Issue 15.*

[5] *Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing", Theoretical Computer Science 560 (2014) 7–11.*

[6] *Marco Lucamarini et.al., "Implementation Security of Quantum Cryptography Introduction, challenges, solutions" (2018), ETSI White Paper No. 27,*

[7] *SECOQC, White Paper on Quantum Key Distribution and Cryptography*

[8] *Makhamisa Senekane et. al., "Six-State Symmetric Quantum Key Distribution Protocol" (2015), Journal of Quantum Information Science, 5, 33-40*

[9] *Mohd Asad Siddiqui, Tabish Qureshi, "Quantum Key Distribution with Qubit Pairs" (2014), Journal of Quantum Information Science, 4, 129-132, http://dx.doi.org/10.4236/jqis.2014.43014*

[10] *Rahman MM et. Al., "Development of Cryptography-Based Secure Messaging System" (2016), Journal of Telecommunications System & Management, Vol 5, Issue 3, DOI: 10.4172/2167-0919.1000142.*

[11] *Ambika R and Hamsavahini R, "A Survey on Hardware Architectures for Montgomery Modular Multiplication Algorithm" (2013), International Journal of Emerging Technologies in Computationaland Applied Sciences(IJETCAS), Vol 5, Issue 3, pp. 217-221.*