Quantum Cryptography and its Application

Shaurya Pratap Singh
Pranveer Singh Institute of Technology, Kanpur

----------ABSTRACT----------

Present cryptography algorithms are based on mathematical problem such as factoring two large prime numbers and N vs NP problem. But computing power and evolution in mathematics increases day by day so it's easy to reverse one way function to quickly such as that of factoring large integers. So the solution is to build a cryptosystem which secure our communication even the computing power is to high so we introduce quantum physics in cryptography which lead to evaluation of quantum cryptography. Quantum cryptography one of the emerging topics in field of computer industry. This paper is an attempt to review fundamentals of quantum cryptography and also analyses few application areas of quantum cryptography and it's limitation.

Keywords-**Quantum cryptography, Quantum physics, Qubit, Quantum key distribution, Photon polarization**

I. INTRODUCTION

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. There are two main branch of cryptography:

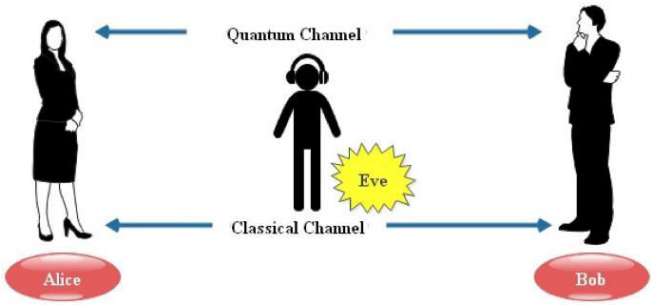
symmetric key cryptography and *asymmetric* key cryptography . In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it encrypts data so that only someone with the right key can decrypt it.

Public –key cryptographic algorithms are widely used in conventional cryptosystems. [1]

Day-by-day we make more and more strong algorithms for securing our sensitive information which is to be transmitted. But the evaluation of speed of computing power work furiously to crack the systems. So for securing it we take help of Quantum laws and introduce Quantum cryptography.[1][2]

Quantum Cryptography came in light when European Union members announced their intention to invest $13 million in the research and development of a secure communication system based on this technology. The system known as SECOQC(Secure communication based on Quantum Cryptography).

In quantum cryptography we use a technology known as Quantum key Distribution(QKD)- is a secure communication protocol method which implement a cryptography protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt message. [2][3]



II. NEED OF QUANTUM CRYPTOGRAPHY

While modern cryptosystem said to be very effective then why lots of money is being spent to develop a new cryptosystem – Quantum cryptosystem?

In current cryptosystem we are using modular arithmetic, discrete mathematics complex prime number calculation and elliptic curve algorithm etc. Such mathematics relies upon one thing- Complexity. In order to secure communication the encryption algorithm must be infeasible. Such algorithms are relatively simple to compute in and direction, yet intangible in reverse without knowledge of another piece of information, typically a number or set of number known as the key.

For as long as the calculation to reverse the cryptographic algorithm take longer than the valuable lifetime of the data it protects, it may be considered secure. But there is a problem we don't know about future, mean none of us can predict what breakthroughs will occur in either the field of computation or mathematics or Physics, numerous mathematician work on problems and also day-by-day system speed also increases.[2][3]

Moore's law seems to be held in place. Traditional computing devices keep getting faster, at rates even wealthiest of us cannot keep up with. The following excerpt from the Intel web site shows this trend in detail:

Moore's observation, now knows as Moore's law, describes a trend that has continued and is still remarkably accurate. It is the basis of many planner's performance forecasts. In 26 years the number of transistors on chip has increased more than 3200 times

from 2300 on the 4004 in 1971 to 7.5million on the Pentium 2nd generation processor.[4]

And it won't stop here. That shows that there is major probability our current cryptosystem will be not secure in future like, **Shor's Algorithm** is a quantum algorithm that factors numbers exponentially faster than the best classical algorithm so it's able to break many cryptosystem but quantum computer are not large enough to currently run Shor's algorithm on modern keys but in future it is possible.

Finally, a new concept in cryptographic security known as Quantum Encryption, which uses Quantum fluctuation of laser light at the physical layer introduced into existing network. It enables ultra-secure communication and near perfect security.

After Max Planck first raised the concept of quantum in 1900, then the theory of quantum mechanics was developed by the 1930s. Quantum cryptography was first proposed by Stephen Wiesner, then a professor in Columbia University in New York, who in 1968 or later, introduced the concept of quantum money and quantum conjugate coding. His seminal paper "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News. In 1984, they produced the "BB84" which is the first quantum cryptography protocol. In 1991, the first experiment prototype based on this protocol was produced which operated over a distance of 32 cm. After sometime it increased to kilometres.[5]

III. WORKIING OF QUANTUM CRYPTOGRAPHY

Quantum cryptography rests on two pillars of 20th century quantum mechanics –the Heisenberg Uncertainty principle and the principle of photon polarization. Quantum cryptography solve the problem of secret-key cryptography
By providing a way for two users who are in different locations to securely establish a secret key and to detect if eavesdropping has occurred. Quantum cryptography doesn't depend upon critical mathematical problem for it's security. In the principle of photon polarization photon have three chosen bases of polarization and the probable result of measurement according to the bases are:

- Rectilinear(horizontal or vertical)
- circular(left-circular or right-circular)
- Diagonal(45° or 135°)

The three bases enumerated above are all conjugate to each other, and this measurement randomization is the fundamental characteristic of quantum particles taken advantage of by quantum cryptography.

The relevant behaviour characteristic which quantum cryptography's resistance to eavesdropping is based on is the Heisenberg Uncertainty Principal. In this most common manifestation, Heisenberg's Uncertainty shows the impossibility of accurately measuring the position and momentum of an elementary physical particle at same time and this principle is the base of Quantum cryptography.
The polarization of a photon can only be measured in terms of a single basis this act of measuring destroy the information necessary to measure polarization with to any other basis. This characteristic allows for two desirable features of a cryptosystem. [6]

1. It is impossible for an eavesdropper to reliable read transmitted data without access to information used to form the transmission.

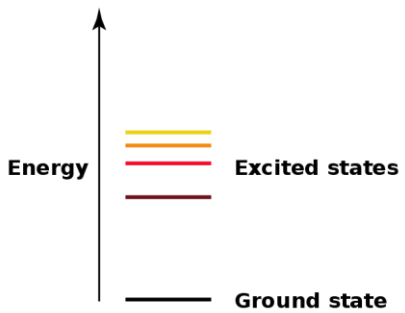
2. Even eavesdropping which desires to be "passive" disturbs the transmission in an unpredictable way. This disturbance is likely to be noticed by legitimate users of the system.

A. Classical bit Vs Quantum Bit(Qubit)

We all are familiar with classical bit which are 0 or 1 and at that time this was the base of any computer and information, all the information was to be translate in classical bit. Quantum Bits also known as qubits are basic units of Quantum computing, just like binary bits for the classical computing.
A classical bit can be in one of the two states 0 or 1, where as a qubit can be in Superposition (in-between) of both of these classical states. [7]
A pure qubit, say $|\psi\rangle$, is represented as the linear combination of two basis states **0** & **1**(for now lets represent them by $|0\rangle$ & $|1\rangle$ respectively)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
where $\alpha, \beta \in [0,1]$, such that $|\alpha|^2 + |\beta|^2 = 1$

For better understanding we take an *example* which explains Qubit, in which we represent bits by energy levels in atom. We can say that the ground state, or the lower one, is called zero and the higher one is called one.
A classical bit mean that my systems will be in one of these two states, so either in the ground state, or in the exited state.
A qubit can be superposition between zero and one that is effectively in the ground and the exited state at the same time.



To construct the qubits, we started from the classical bits as vectors. And these vectors have a special name, namely we call them the standard basis, or sometimes also the computational basis, and alpha and beta are called amplitudes.

B. Quantum Key Distribution:-

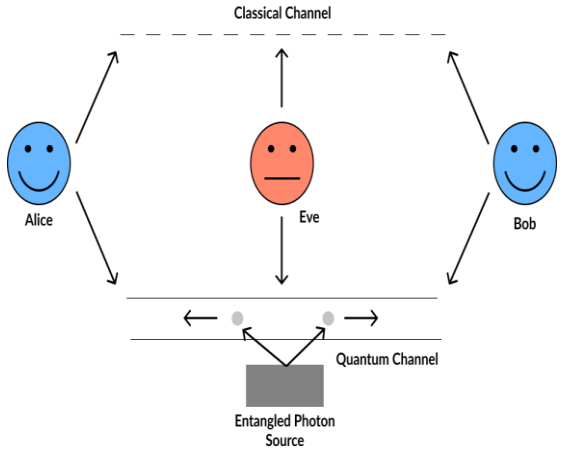
The goal of Quantum Key Distribution (QKD) is to share a string of random bits between two parties, using quantum technologies and ensure that only the two parties are able to know the message or string.

a) How does QKD Work?

The security of QKD is based on fundamental characteristic of quantum mechanics. The act of measuring a quantum system disturbs the system. Thus, an eavesdropper trying to intercept a quantum exchanging particles can decide either to discard the corrupted information or reduce the information available to the eavesdropper to nought by distilling a shorter key.

A QKD implementation typically includes the following components:

- A fibre or free-space quantum channel to send quantum states of light between the Alice and Bob(transmitter and receiver). This channel does not need to be secured.
- A public but authenticated communication link between the two parties to perform post-processing steps and distil a correct and secret key.
- A key exchange protocol that quantum properties to ensure security by detecting eavesdropping or errors, and by calculating the amount of information that has been lost.



Both error and potential information leakage are removed during subsequent error correction and privacy amplification post-processing steps, leaving Bob and Alice with a shared key known only to them.

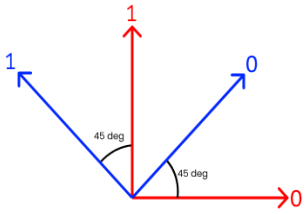
b) Type of Quantum Key Distribution:-

In Quantum cryptography a variety of protocols have emerged and been demonstrated in many real-world scenarios.

The first approach is discrete variable QKD, which encodes
quantum information in discrete variable and uses single photon detectors to measure the received quantum states. Example is the BB84.

a. The Oldest Protocol:BB84

BB84 protocol, proposed in 1984 by Bennett and Brassard – that's where the name comes from. The idea is to encode every bit of the secret key into the polarization state of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be 'fragile' and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarization state. This will lead to errors, and again the eavesdropper will reveal herself.



The protocol then runs as follows. Alice sends a sequence of pulses (for instance, femtosecond pulses with 80 MHz rep. rate), each of which, ideally, contains a single photon polarized differently. Alice encodes zeroes into H-polarized photons while unities she encodes into V-polarized photons (red arrows in Fig). But this happens only in half of the cases. The other half of bits, chosen randomly, are encoded using a diagonal polarization basis (blue arrows in Fig). Then, the 'D' polarization corresponds to zero and the 'A' polarization, to unity. The receiver, Bob, measures the polarization using a standard setup (a PBS or a Glan prism with two single-photon detectors in the output ports, or a calcite crystal also followed by two detectors). This way Bob can distinguish between H and V polarizations if he uses the HV basis (further denoted as '+'). But in half of the cases Bob randomly changes his basis (the orientation of his prism) to AD (denoted as 'X'). After a certain number of bits has been transmitted (and all photons have been detected and destroyed!), Bob publicly announces which basis he used for each bit. Alice then says in which cases they used the same bases. They throw out the bits where they used different bases, and leave only those where they used the same one. After this procedure (key sifting) the length of

the key is reduced twice, but what remains is random and coincides for Alice and Bob.
Then, they check if there was eavesdropping. To this end, they take a part of the key for instance, (10%) and compare it. This procedure is also public, but these 10% are then discarded. If the Fig.1 eavesdropping took place, the key would contain errors. Then the whole key is thrown out and the procedure is repeated again. The table below gives an example of transmitting 8 bits of a secret key. After the key sifting, only 4 bits are left.[8][9]

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	**X**	+	+	+	X	+	X	**X**
Photon polarization Alice sends	**D**	V	**V**	H	A	**H**	D	**A**
Bob's random measuring basis	**X**	X	+	X	+	+	+	**X**
Photon polarization Bob measures	**D**	D	**V**	A	V	**H**	V	**A**
public discussion of basis								
Shared secret key	0		1			0		1

One does not have to use polarization; it is also possible to encode the bits into the phase of single photons. But the advantage of polarization is that it is conserved rather well in the course of light propagation through the atmosphere. Now, the largest transmission distance is from a satellite to a ground station, ~1200 km. An important question is how to produce single photons. One way is to use light emitted by single atoms, molecules, colour centres in diamond, or quantum dots. However, this requires a lot of effort and does not provide 'on demand' photons; with an account for emission and collection efficiency, these emitters are still probabilistic. In practice, one still uses weak coherent states (with the mean photon number per pulse ~0.2-0.3).

A second approach is continuous-variable QKD (CV-QKD). In this approach, the quantum information is encoded onto the amplitude and phase quadratures of a coherent laser, and can then be measured by the receiver using homodyne detectors Examples protocol include Silberhorn(2002) Grangier(2003).

Both of these approaches have been proven to be information-theoretically secure even in the presence of an attack or eavesdropper.[9]

c) Detecting Eavesdropping

To detect the eavesdrop; polarization of the photon is to be measured. The key concept is that it is impossible to measure the polarization of the photon without destroying it. So if Eve intercepts the signal, she will have to send new photons to the receiver so that she may not be detected about her presence. However, she will inevitably introduce errors, since she doesn't know the state and polarization. So Alice and Bob can check for errors by revealing a random subset of their generated sequence and comparing it publicly. If they are not satisfied with the error rate, they can set up a different channel. This ensures that while Alice and Bob cannot stop Eve from listening in, they would always know that she is there. In entangled photon transfer method can also be used for this purpose. According to physics law, a change in the polarization of one photon in a pair will affect the other one, no matter how far apart they are. In order to eavesdrop, Eve would have to detect one of the photons and measure it, thus destroying half of the pair. This act will end the quantum relationship of the two members of the pair, which is very easy to detect by Alice and Bob, and impossible to reverse for Eve. Without revealing the specific results of their measurements, the sender and the receiver can talk publicly and see where intervention has occurred. [6]

IV. ATTRIBUTES OF QKD

QKD offers an agreement based on a shared random sequence of bits in between two distinct devices/users, with a very less probability of other devices (eavesdroppers) being able to make successful inferences. In practice, such sequences are used as secret keys for encoding and decoding messages between the two devices/users. In this view, QKD is quite clearly a key distribution technique, and one can rate QKD's strengths against a number of important goals for key distribution, as summarized below.

1. Confidentiality of Key

Confidentiality is the main attribute in QKD. Public key systems have an uncertainty that decryption is mathematically intractable. Hence key agreement primitives are widely used in today's Internet security architecture, which may perhaps be broken at some point in the future. This could not only hinder future ability to communicate but could reveal past traffic. Classic secret key systems suffered from various problems, namely, insider threats, logistical burden of distributing keying material. Assuming that QKD techniques are properly embedded into an overall secure system, they can provide automatic distribution of keys that may offer security superior to that of its competitors.[10]

2. Authentication

It is crucial for security to authenticate some (or all) of the classical messages communicated during the public discussion. We will explain why this is the case, how authentication is achieved and what type of authentication must be used in the following sections.

3. Distances and Location Independence

This feature is notably lacking in QKD, which requires the two entities to have a direct and unencumbered path for

photons between them, and which can only operate for a few tens of kilometers through fiber. Resistance to Traffic Analysis Adversaries may be able to perform useful traffic analysis on a key distribution system e.g., a heavy flow of keying material between two points might reveal that a large volume of confidential information flows, or will flow, between them.[10][9]

V. APPLICATION OF QUANTUM CRYPTOGRAPHY

Here are some current and future near application of quantum cryptography.

i. Quantum Money

In the first paper of Quantum Cryptography, written by Stephen Wisener, there was a proposal for quantum money or money that is physically impossible to copy.
According to the Bank of England, a small fraction of the banknotes circulating in the UK are counterfeits (around 0.02%), representing around 10 million pounds of fake and worthless money.
Another reason to be interested in Quantum Money is the potential security breach in crypto-moneys. The most famous crypto-money is Bitcoin, and it has been more used in the last few years. The issue is that in the end, The Bitcoin (an other crypto-moneys) relies on public-key cryptosystems that could be become insecure with quantum computational power.
We will briefly see several implementation of quantum money here, but all of them have the requirement of quantum memory that can store the quantum states for a long time, which is not yet possible but in future may be it is possible.
There are two categories of quantum money:

- Private quantum money: only the bank can verify that the money is no counterfeit;
- Public quantum money: anyone can verify that the money is no counterfeit;[11]

ii. Quantum Voting

Quantum voting can be interesting to study. Also, it shows far quantum principle be used in cryptography protocols.
There various protocol like BB84, which help to achive quantum voting and it's enable some features:

1. Only the vote of authorized voters can be taken into account;
2. Every interested voter must vote exactly once
3. No one can control other voters opinions about the issue to be voted upon;
4. No one can change the votes of the other voters from being detected by the administrator and the other voters;

But it is clear that Quantum voting will not be used for large scale votes before a pretty long time, and that for two reasons:

- It would very expensive in quantum resources,
- It is not possible to expect the public to understand quantum physics, and they cannot trust something they don't understand.

iii. Quantum Internet

Today's internet is relatively fast, but its security is paltry compared to quantum-encrypted transmissions. Quantum encryption would greatly slow down the internet. In the future, however, it's possible that we could switch effortlessly between "regular" and "quantum encrypted" internet, so that our most sensitive transmission would be passed along in an ultra-secure manner. This would achieve
the ideal of simultaneously fast and secure internet.[11]

VI. CONCLUSION

In this paper we are seeing the use of Quantum cryptography and how quantum mechanics involves in this cryptosystem. We have first discussed about quantum key distribution, which is the first application of quantum physics in cryptography if we omit the unnoticed propositions of WIESNER. In this paper we also know about why Quantum cryptography needed. And we discussed about a key exchange using a satellite was performed between two points on Earth separated by 7600 km Finally, schemes based on BELL's inequality violation were proven useful to do device independent quantum key distribution. Next, we went beyond QKD and explore quantum public cryptographic tasks: public-key, digital signatures, and fingerprinting. It shows the range of possibilities and how we can extend Quantum Cryptography. However, it seems that these tasks require a lot of resources, and sometimes devices that are not available today. Finally, we presented other quantum cryptographic tasks. Quantum randomness is already commercialised while the other tasks do not seem attainable today (quantum money requires long term quantum memory for example). One thing we could talk about in this section are quantum voting, which is an extension of the classical voting, and have some interconnections with Quantum Cryptography.
QKD provides significant advantages when compared to conventional key distribution. First, the security of QKD security rests on the foundations of quantum mechanics and this make it more secured. This is in stark contrast to traditional key distribution protocols which rely on computational security, where the computational difficulty of certain mathematical functions is the foundation of security. Second, when using QKD, one can determine if an adversary is eavesdropping on the link because it will induce errors in the key exchange process. In contrast, traditional key exchange algorithms cannot provide any indication of eavesdropping or guarantee of key security. Quantum cryptography will be very important not only in cryptography and allied areas [12-20] but also in wireless

communication scenarios [21-26] and various network security applications [27-31].

REFERENCES

1. Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008
2. Diffie W, Hellman M. New Directions in Cryptography. Stanford University; 1976. 40 p
3. Jones A Z. What Is a Quantum Computer? [Internet]. About.com-Physics; 2009 Mar. 11. [cited 2009 May 3].
4. By Gordon E. Moore "Cramming more components onto integrated circuits"
5. Wiesner, Stephen., 1983. "Conjugate coding." ACM Sigact News 15.1: 78-88.
6. By Jigsaw " What is Quantum Cryptography and How it Works?"
7. By Universite de Montreal, Montreal. Canada, "A Study on the basics of Quantum Computing".
8. By Air Force Institute of Technology, "Quantum Key Distribution: Boon or Bust?"
9. By N.Sasirekha, M.Hemalatha, " Quantum Cryptography using Quantum Key Distribution and its Applications"28
10. By Alan Mink, Sheila Frankel and Ray Perlner "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration"
11. By Yi Zhao "Quantum Cryptography in Real-life Applications: Assumptions and Security"
12. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6, DOI: 10.1680/jnaen.18.00006
13. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451, DOI: 10.1080/09720529.2019.1692450
14. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38, DOI: 10.5120/ijca2015906060
15. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9, DOI: https://doi.org/10.1007/s11277-020-08008-4
16. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720, DOI: https://doi.org/10.1007/978-981-15-4692-1_54
17. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5, DOI: 10.1109/CICT48419.2019.9066168
18. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5, DOI: 10.1109/UPCON.2018.8596905
19. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7, DOI: 10.5120/cae2017652680
20. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6, DOI: https://doi.org/10.48550/arXiv.2203.12606
21. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86, DOI: 10.1109/UPCON.2016.7894629
22. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21, DOI: 10.5120/cae2015651903
23. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39, DOI: 10.5120/ijca2015906437
24. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419, DOI: 10.35940/ijrte.B1503.078219

25. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

26. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

27. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

28. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

29. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI:https://doi.org/10.1080/09720529.2021.1932902

30. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

31. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI:
https://doi.org/10.1080/09720529.2021.1932908