IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 4, Ser. I (Jul. – Aug. 2020), PP 58-64
www.iosrjournals.org

Network Security Cryptographic Protocols and Lattice Problems

Dr.Daruri Venugopal
Professor, OPJS University, Churu,Rajasthan,India.

Abstract:*In this Research investigation we présent new results in two areas – Cryptographic protocols and Lattice Problems. We introduce a new Protocolfor electronic cash which is exclusively designed to fonction on hardware with limited computing power. The approche has provable Security properties and low coputational requiremnts, but it still gives a fair amount of privacy. Major feature of the system is that there is no master secret that could be used for counterfeiting money if stolen. In this Research content we introduce the notion of hierarchial group signatures. In Merchant transactional process the signer that is as similar as a leaf of the sub tree of a group manager, the group manager learns which of its children that manages the signer. We introduced few practical conditions that are suitable for the new notion and construct a scheme that is provably secure given the existence of a family of trapdoor permutations. We also present a construction whcih is relatively practical, and prove its security in the rand om oracle model under the strong RSA assumtion and the DDH assumption. We déterminea simple and efficient system for electronic cash withprobable Security properties. The system relies on symmetric encryption technlogies rather than asymmetric.*

Key Word*:Asymmetric, Cryptographic protocols, electronic cash, Counterfeiting, encryption, signers, trapdoor.*

Date of Submission: 14-07-2020 Date of Acceptance: 29-07-2020

I. Introduction

When a word Cryptography is mentioned what first comes to mind is probably sending secret messages. This is justified, as hiding information for confidentiality. An analogy is to send a message in a sealed envelope , or in safe mode. The analogy here is to sign a paper with the message on it. Since signatures are assumed tobe hard to forge, a signature identifies the sender. Since we want the system to be secure, we want it to be infeasible to compute any useful information about the plaintext from the cipher text, provided that they key‘ k’ is unknown. Consider the functions necessary to ensure that a message is not counterfeited or modified. The usual approach is to define a function S to create a message authentication code MAC and a function ‘V’ to verify that a MAC is valid. Today a large and growing part of payments are made by electronic means, but there is still much room for improvement. Credit cards may be suitable for large amounts, but for small amounts the cost of using a credit card is too high.

The purpose of electronic cash is to give an alternative option for payment which provides some anonymity to the customer, and possibly avoids the need for contracting the bank for every transaction. In this research content we present a system for electronic cash that is purely based on symmetric primitives. Themajor advantage of this is that we get a system where the coins are in small denomination and where the cryptographic functions performed by the customer requires little processing power. The system relies on symmetric encryption technologies rather than a symmetric. This enhances performance, and the system will gives a fair level of anonymity.

II. Cryptography Asymmetric Encryption Schemes

Asymmetric systems use two keys, the public key and the private key known as P_k and S_k respectively. In Cryptography Asymmeric Schemespublic key is used for encryption and the private key is used for decryption. The public key can be published, since it is used only for encryption, but the private key must be kept secret. Similarly if we compare this with symmetric cryptosystems to see what the differences may mean in practice. Assume ten people work at the same company, and that they want to be able to send encrypted messages to each other. First consider a symmetric cryptosystem.

In Such type of stages one solution is to have a single common key that everything is encrypted with but there are several drawbacks with this approach. Someone who gets hold of the key is able to read all message sent. A second solution is to have one key between every pair of employees. Then only the intended recipient can read his messages, and if one employees sells his keys, only the messages sent or received by that employee can be read. However, the number of keys necessary for such a system is high.

It is clear that Our ten employees need a total of 45 keys . The number of keys are not that much high but we must take into account that agreeing on a symmetric key is a cumbersome task. It is not suggestible any manner to select keys electronically, since they can be dropped and if a key is sent by mail, there is always the risk that some one opens the envelope and gets the key. The only safe mode is to meet in person. Now consider a company with 1000 employees. Then a total of 499,500 keys are necessary. It is obvious that symmetric cryptosystems have certain drawbacks. We can solve this problem using symmetric cryptography approach method. Each of the ten employees generates a key pair consisting of a private and a public key. The public keys are quoted in the company phone book. If A wants to send a message to B then A looks up B in the phone book, encrypts using public key and sends the message. We can identify that No keys have to be exchanged under secure conditions.

III. Building Cryptographic Protocols

Considering the Digital Signatures – authenticity can be achieved by asymmetric means. When a MAC is used, the same key is used for computing the MAC. Therefore only the intended recipient can check the validity of the message. We can identify the ability to compute a MAC making it hard to use a signature as proof in case of a dispute. Therefore, in many situations, it is desirable to have a scheme in which it is possible to verify without being able to sign. Using asymmetric techniques we can construct a scheme where the signing is performed using the private key Sk and the verification with the public key Pk. Now it must hold the $Vpk(m.Ssk(m)) = 1$.

This is also what we expect from real-world signing schemes- anyone can look at a signature and check whether it has been written by the sender , but the sender also should be able to produce such a signature. A digital signature is in one sense more secure than a physical signature on paper. When a paper with the message written on it is signed, it is hard to ensure that the message is not altered afterwards. A forger may add new text to a signed document or combine pages from two or more signed documents into a new document. A secure digital signature scheme withstands attacks of this type, since the signature is tied to the message and becomes invalid if the message is modified. Two of the most important building blocks for cryptographic functions are one way functions. We can consider the situation as the functions that are easy to compute but hard to invert, trapdoor functions.

Functions that are one way functions with the additional property that there is a secret which makes the function easy to invert Take, for example, multiplication operation. It is easy to multiply two numbers, but no method is known that factors a numbers into its prime factors in reasonable time. It should be noted that the existence of one way and trapdoor functions is a classical open problem, and a proof of their existence would be a major breakthrough. There are functions that have been subject to intensive investigation for more than thirty five years, and no evidence contradicting the hypothesis that they are trapdoor functions have been found. It is therefore reasonable to assume that they are indeed trapdoor functions. From functions that are assumed to be trapdoor functions, it is possible to build cryptographic primitives, e.g., encryption and signature schemes.

To achieve more complex tasks, such as setting up a secure channel between parties who have not previously met or crating digital coins, we need to describe how to combine primitives to get the functionality we need. The result is called a protocol, and the protocol describes how the participants should act. A protocol can be seen as a set of algorithms, one for each participant.

A protocol may be interactive or non-interactive. An interactive protocol is used when the parties can send messages to each other in an interleaved manner. An example may be a use logging on to a website. In a non-interactive protocol the sender creates the message on his own, and only then sends it to the receiver. Encrypting and singing emails area typical examples of non-interactive protocols.

IV. EFFICIENT Vs Practical Protocols

In regular process we want our protocols to be as good as efficient. However, in different contexts efficiency may have different meanings. The common definition of an efficient algorithm is that the execution time. It is determined that execution time is bounded by a polynomial in the size of the input. If we consider the grade school algorithm for multiplication is polynomial time, since the number of steps needed is less than $2n^2$, where n is the number of digits of each factor. An example of an algorithm that is not polynomial is factoring by exhaustive search. To factor an n-bit number 'm' we may need to check each number up to $\sqrt{m}$, that is $2^{(n/2)}$ different numbers. Even if we assume that we can check divisibility in a single step, we still need an exponential number of steps before we are guaranteed to have a result. It is clear that this definition of efficient algorithms does not cover everything we need from an algorithm to be usable in practice. If we design an algorithm that runs in n^{30} steps , it would still be considered efficient according to the above definition. However, the algorithm would be impossible to use in practice except for extremely small inputs.

In this investigation we focus on protocols that are not only efficient in the above meaning, but that are practical. Therefore the protocols must be specified in such detail that it is possible to analyze their running

time precisely and not only show that it is bounded by some polynomial. Practicality is not a well definition as per the research process. In some cases, we want a protocol that can be executed on devices with little computing power such as smart-cards or mobile phones. In other cases it is enough if the protocol runs reasonably fast on a personal computer, and in still other cases the protocol will run on a server with large storage capabilities.

V. Security of Cryptographic Primitives and Protocols

In Security we want the cryptographic primitives as mandatory. However, we need to define precisely what we mean by security of a primitive in such type of Protocols. Let us consider an encryption Scheme. One definition of security is that the scheme is secure if an attacker who sees a cipher text cannot recover the plaintext. However, in some scenarios this is not enough, since the attacker may have access to additional information. In such cases may be the attacker knows that the plaintext is either 'YES' or 'NO' stages and may be the attacker has seen encryptions of other plaintexts. Some times the attacker even has seen encryptions of 'YES' and 'NO'. A good cryptosystem should remain secure even under these circumstances. For example to remain secure even if the attacker knows encryptions of YES and NO the encryption must be probabilistic.

VI. Anonymity

Selecting and designing protocols that are as secure as theprimitives used is not trivial in Anonymity cases. It may very well in such cases protocol turns out to be insecure although all components used are secure. Considering a suitable example for the case such that a scheme for electronic cash involving customers, merchants and a bank, naturally a customer should not be able to counterfeit money, but what happens if a customer and a merchant collaborates to produce counterfeit money? Or may be when two customers together try to create a coin that appears to be valid to the merchant but which is rejected by the bank ? Obviously there are many suitable details when deciding what kind of security we want from a protocol. Therefore it is important to make a clear definition of security and to prove that the protocol fulfills those definition under some possible assumptions. Assume the cash we withdraw had our name on it. What would that mean ? In most cases it would not mean anything. Non one would be interested in knowing that it was you who bought that pack of chewing gum. We might feel a little bit uncomfortable if you knew that a curious trainee working in the pharmacy can keep track of what medicine we use. If we purchase a newspaper with cash, it is not possible to trace the purchase back to you by looking at the coins you paid with. If you buy a couple of tokens for the metro, it is not possible to see if two trips were paid by tokens purchased at the same time. The common reason neither coins nor metro tokens are traceable due to non available of serial number on it.

The major reason they did not have a serial number is that their low value do not make them an interesting target for counterfeiter the cost of producing a fake coin or metro token probably exceeds its value. Now we may argue that these transactions are not at all anonymous, if we go and buy the newspaper in person, anyone can see what we bought. However, the important point here is that it requires considerable resources to track a person that way, and it is impossible to do in an automated way on a large scale. When the physical coins and metro tokens are replace with electronic counterparts, the scenario is changed. The cost of copying an electronic coin, which is nothing but a sequence of zeros and ones, is next to nothing. Therefore even low value coins need some kind of serial number to detect duplicates, and that potentially makes them traceable. One of the challenges when designing protocols for transactions that people assume to be anonymous is to make them anonymous also when performed electronically.

Before we design anonymous protocols, we must decide what we mean by anonymity. One definition of anonymity is that a transaction cannot be connected to the identity of any involved party. This definition, however, is weaker than the anonymity of real world transactions, because it does not say anything about connecting transactions. If the coins are anonymous only in the above status the identity of the buyer of the newsletter may still be revealed if the two purchases can be connected.

If a protocol involves several parties, in the case of electronic coins a customer, a merchant and the bank, we may settle for anonymity only towards the merchant to make the protocol more efficient. In other words, the merchant cannot link two purchases, but once the coin reaches the bank, the bank can see who withdrew the coin. Another concept is revocable anonymity. Here some trusted third party can extract the identity from a coin, but otherwise the coin is anonymous towards both the bank and the vendor. Although anonymity is desirable from the user's point of view, protocols that ensure anonymity tend to be less efficient than non-anonymous protocols. Also from a legal point of view anonymity might be problematic. If electronic coins are achieved through black mailing or other illegal activities, anonymity works in favor of the criminal. In an anonymous scheme for electronic coins the bank cannot monitor the flow of coins. It will detect irregularities only after a long period of time. This may be one reasons why the schemes for electronic cash that are in use are non-anonymous.

VII. Payment Systems

When making purchases, the most common ways to pay for the goods is either by using cash or by using a payment card or check. Cash has the property that it is anonymous and that it is possible to verify that it is valid by just looking at it and without calling the bank. This offline property of cash is important, and very desirable. It reduces communications costs, it makes the scheme more robust since it does not require the bank to be available, and it is fast. The merchant can deposit the cash with his bank, use it ias change, buy goods pay salary etc.

A payment card on the other hand is not itself a proof that the customer has the money to pay. The issuer must be contracted to verify that the customer has the necessary funds, but once the transaction is completed, it cannot be stolen like cash. Since the merchant's name is part of the payment, no-one else can get credited for the transactions. Systems for digital cash try to keep the anonymity of the customer, possible with a trusted party that can revoke the anonymity. However, since a digital coins is just a bit-string, it can be copied and spent twice.

The most common way to deal with this is to design the system so that the identity of the owner is revealed if the same coin is spent twice. Another solution is to make the system online, but then part of the motivation to use coins is lost.

Systems for digital cash often require that the merchant deposits the cash with the bank after the transaction rather than reuse it. However, digital cash may also have the useful property that it cannot be stolen while at the merchant, since the merchant's name is part of the transactions. If digital cash does not completely correspond to cash in the real world, payment card transactions are easier to make purely electronic. In many cases this simply means that the physical signature on the receipt is replaced by a digital signature by the cardholder. Here, however, we can ask for more and make payment through card transactions anonymous towards the merchant. The goal then is to design a system such that two transactions cannot be linked by the merchants. The system will still be non-anonymous towards the issuer, since it must be able to charge the correct account. A trivial way to achieve anonymity towards the merchant is to give each cardholder not just one card number, but several one-time numbers. The bank keeps a list of which number belongs to which cardholder, and the cardholder makes sure each number is only used once. Provided that the card numbers are generated randomly, such a system would be anonymous towards the merchants.

VIII. Group Signatures

In this Section we discuss a more general approach to the problem of creating anonymous credit cards. We use the concept of group signatures. In a group signature scheme, there are group members and a group manager. Group members can sign documents on behalf of the group, but the only information that someone other than the group manager. Identity of a signer is determined by the group manager. As the alert reader already has seen this is exactly what we need to make payment cards anonymous. The group members are the cardholders, and the issuer is the group manager.

When making a payment the cardholder produces a group signature on the transaction. The merchant verifies that the signature is produced by someone in the group of cardholders, but does not get any additional information. When the transaction is passed onto the card issuer, the issuer, who acts as group manager, extracts the identity of the cardholder to debit the correct account.

The Scheme described above with group signatures works for payment cards when there is just one issuer, and every merchant sends all transactions directly to that issuer. In reality this is not the case. There is not just one but several issuers cooperating within a network. Rather than sending the transaction directly to the issuer, the merchant sends it to the network, which routes it to the issuer. The obvious way to solve the problem is to set up a group signature scheme for each issuer. With this result we lose some anonymity, since the merchant learns the name and other details of the issuer, and in some cases this can give quite a lot of privacy information.

Therefore we would like a variant of group signatures where there are group managers that only get partial information about the identity of the signer. More specifically, in the case of payment cards, we need a scheme such that the signature is anonymous to the merchant, the network can see which issuer the card belongs to, and the issuer sees the identity of the cardholder. Naturally this can be generalized so that there are several intermediate group managers that get more an more detailed information about the identity. In this research we describe such an extension of group signatures.

IX. EMV Payment Cards

Transactional mode we can identify that majority of payment cards are equipped with a magnetic stripe where the cardholder data is encoded. Although a convenient and cheap solution. It has its security problems. The magnetic stripe can be copied and modified, making it a good target for counterfeit and fraud. The

transactions made with a magnetic stripe are not digitally signed, making it possible to modify the transaction data after the transaction took place.

One alternative to the magnetic stripe is smartcards. A smart card is a tiny computer placed on a plastic card. As with any computer, it can store and process data. This is a very useful property to prevent copying and modification of cards. Since the amount of money lost on fraud by the payment networks is growing, there is an ongoing program to switch to smart cards. The switch is currently in progress, with some issuers already issuing smart cards and some still using the magnetic stripe.

With smart cards, the security is increased considerably. A smart card cannot be copied or modified the same way a magnetic stripe can. It can hold secret data used only internally by the card. Smart cards can sign transactions, thus ensuring they care sent to the payment network unmodified. Some smart cards also contain a private key for authentication purposes. Since the private key is accessible only to the internal smart card software, such a cad cannot be duplicated.

Cardholder data on a smart card may be digitally signed by the issuer, preventing it from being modified as data on the magnetic stripe. With the magnetic stripe a cardholder can pay wherever his brand of card is accepted. He does not have to worry about who manufactured the terminal or which bank will process the payment, since all magnetic stripe cards and all terminals work according to the same standards. For the switch to smart cards to be successful, the same interoperability is necessary also for smart cards. Therefore an international, publicly available standard called EMV has been developed.

X. Cryptography and Lattices

In this Research Paper we point out a vulnerability in some EMV cards. Although the EMV standard builds onprimitives in which no vulnerabilities are known, we show that certain EMV card configurations are insecure. The vulnerability would allow an attacker to use any EMV card to perform an unlimited number of offline transactions.

EMV does allow for offline transactions, but there is a limit on the maximum number of consecutive offline transactions stored on the card. To design cryptosystem we need hard problems with minimum requirements for examplelattice problems.

A lattice is defined as the set $(\lambda_1 b_1 + \lambda_2 b_2 + \lambda_3 b_3 + \ldots\ldots\ldots\ldots + \lambda_n b_n)$ where λ_i are integers and $b_i \in R^n$

The lattice consists of points in R^n which are also known as lattice vectors generated by adding combinations of the basis vectors with integral coefficients. In below Fig.1 a basis for a two dimension lattice is shown together with the lattice points generated by the lattice.

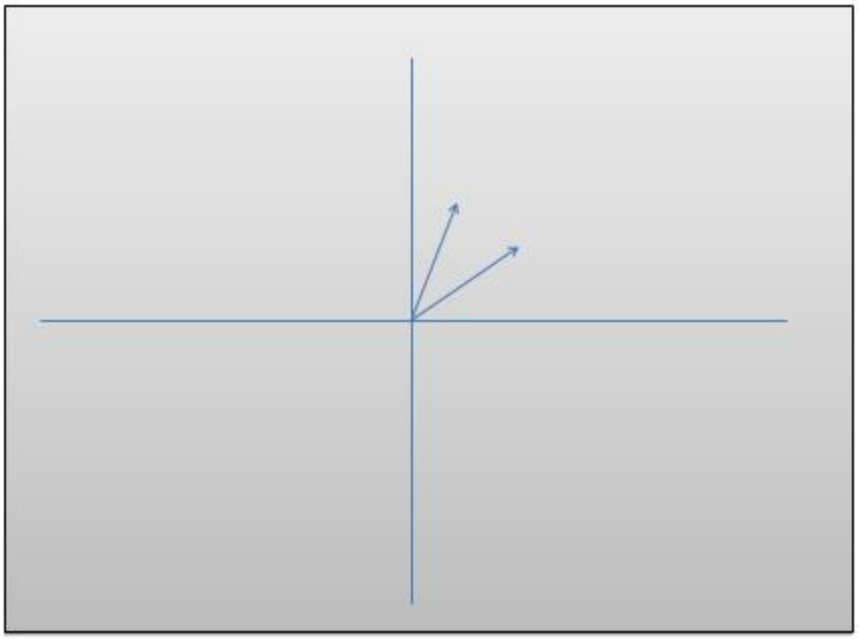

Fig 1: A two dimensional lattice

In the below Fig.2 shortest vector in the two dimensional lattice is marked, and here we see that in general the shortest vector is not one of the basis vectors, and that the shortest vector is never unique, since if 'V' is a lattice vector then it is denoted as V'.

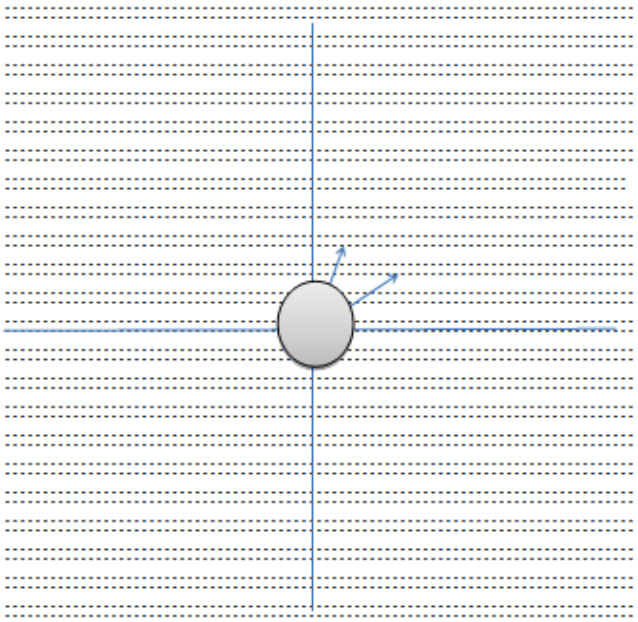

Fig.2 The Shortest vector in the lattice

Computing a shortest vector in a two dimensional lattice is not difficult, but in lattices of higher dimension the general consensus is that no algorithm which efficiently solves SVP exists. Now, if we cannot expect to find the shortest vector in reasonable time, it is natural to ask if we can find a vector which may not be the shortest but which is not too much longer than the shortest.

In turns out that the answer to this question depends on what one means by "not too much longer" . It is known that finding a lattice vector that is up to a factor 'k' longer than the shortest is for any constant k. On the other hand there is an efficient algorithm that is known to always give a vector that is at most $2^{(n/2)}$ times as long as the shortest vector, and that in practice often produces even better results. It is still unknown precisely where the border lies between what can be computed efficiently and what cannot.

Lattice problems have cryptographic applications . It is known that the crypto-system NTRU would be insecure if short vectors could be found in a certain type of lattices. Since the NTRU lattices are of very high dimension, it is believed to be infeasible to find such sort vectors. However, the NTRU lattices have acertain structure that could potentially make them weaker. In this Research part we can understood the structure and show that the SVP is not easier in this type of lattices. Our approach is to show that given an arbitrary lattice ω_1, it is possible to compute a lattice ω_2 which has the special structure and lies very close to ω_1. Now we can conclude that if SVP were easy in ω_2, then it would be easy in ω1 as well, since a solutionto SVP inω_2 can be translated into a solution in $\omega_1$as well. There fore the special structure of $\omega_2$does not help when solving SVP.

Fig.3. Approximating a lattice with another lattice

XI. Conclusion

In this Research paper we introduced and the new results in Two areas Cryptographic protocols and lattice problems. Presented a new protocol for electronic cash which is designed to fucntin on hardware with limited computing power. The scheme has provable security properties and low computational requirements, but it still gives a fair amount of privacy. A new and well defined feature of the system is that there is no master secret that could be used for counterfeiting money if stolen. We introduced the notion of hierarchical group signatures. This is a proper generalization group signatures, which allows multiple group managers organized in a tree with the signers as leaves. For a signer that is a leaf of the sub tree of a group manager, the group manager learns which of its children that manages the singer. We provided properties for the new notion and construct a scheme that is provably secure given the existence of family of trapdoor permutations. We introduced and analyzed basic properties - weakness in the specification for a offline capable EMV payment cards. The weakness which applies to cards without RSA capability, enables an attacker to duplicate a card and make transitions that cannot be tied to the original card.

References

[1]. J.Camenisch.Efficient and generalized group signature. In Advances in Cryptozoology – EUROCRYPT-97, Vol.1233 of Lecture Notes in Computer Sciences, Pages 465-479,Springer Verlag,1997.
[2]. J-Y Cai and A,Nerukar, An improved worst case to average case connection for lattice problems. In 38th IEEE Symposium on ACM Symposium on the Theory of Computing (STOC), pages 468-477. IEEE Computer Society Press,1997.
[3]. L.Chen and T.P.Pedersen, New group Signature schemes. In Advances in Cryptology, Springer Volume 1994.
[4]. R.Cromer, I Damgard, and B.Schoenmakers. Proofs of partial knowledge and simplified diesing of witness hiding protocols. In Advances in Cryptology – CRYPTO-94 volume 839 of Lecture Notes in Computer Science, Pages:174-187, Springer Verlag,1994.
[5]. The proth search page: http:// www.prothsearch.net,March 2004.
[6]. D.Pointcheval and J.Stern. Security arguments for digital signatures and blind signatures, Journal of Cryptology 13(3):361-396,2000.
[7]. Bellovin,S. and Cheswick,W. " Network Firewalls ". IEEE Communicatins Magazine, September 1994.
[8]. Bellovin, S and Merritt, M. " NIDX – An Expert System for Real Time Network Intrusion Detection". Proceedings, Computer Networking Symposium,April 1988.
[9]. Bace,R., and Mell, P.Intrusion Detection Systems. NIST Special Publication SP 800-31, November,2000.
[10]. Bellare, M; Canetti. R: and Krawczyk, H. " Keying Hash Functions for Message Authenication". Proceedings CRYPTO-Aug-1996, Published by Springer Verlag.
[11]. Chess, D. " The Future of Viruses on the Internet". Proceedings,Virus Bulletin International Conference, October 1997.
[12]. Chapman, D. and Zwicky, E, Building Internet Firewalls, Sebastopol, CA : O'Reilly, 2000.
[13]. Davies, C., and Ganesan, R, BApasswd: A New Proactive Password Checker". Proceedings 16th National computer Security Conference, September 1993.
[14]. Anderson, J. Computer Security Threat Monitoring and Surveillance. Fort Washigton, PA: James P.Anderson Co., April 1980.
[15]. Bace, R.Intrusion Detection. Indianpolis, IN:Macmillan Technocal Publishing,2000.

Dr.Daruri Venugopal. "Network Security Cryptographic Protocols and Lattice Problems." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(4), 2020, pp. 58-64.