A Key-Ordered Decisional Learning Parity with Noise (DLPN) Scheme for Public Key Encryption Scheme in Cloud Computing

Tarasvi Lakum[1]
Department of CSE
Koneru Lakshmaiah Education Foundation
Vaddeswaram, A.P, INDIA

B.Thirumala Rao[*, 2]
Department of CSE
Koneru Lakshmaiah Education Foundation
Vaddeswaram, A.P, INDIA

***Abstract*—The variation of decisional learning parity with noise (DLPN) named as key-Ordered DLPN based security algorithm is presented in this work. The proposed scheme uses DLPN by extending it to an even-odd-order scheme, depend on the value of probability distribution of odd and even bits for encryption, where odd and even bits are the input integer values for key generation algorithm. This states that the probability distribution of odd and even bits are ordered based on the key generation, the process of odd and even bits resolving is the solution of DLPN attacker problems, thus, the proposed scheme provides more correctness and security proof. Through the learning parity with noise (LPN), DLPN and RSA algorithms, the proposed system is evaluated, to measure the encryption time, public key and ciphertext bits.**

***Keywords*—LPN; DLPN; RSA; key-ordered; time**

I. Introduction

To provide data security, in a confidential and in an authorized encryption, there is a need of protection to the information from an unauthenticated user [1-3]. The information required should be made available to the authorized users and to be protected from unauthorized users by creating it unavailable. Through which the availability, confidentiality and integrity of data become necessary for the security of data.

Recently, an encrypted security [4] [20-21] became an ideological research area, with a process of keeping the data in a server and encrypted form of data is communicated, in a way for the purposed users can have access and process. Cryptography broadly made in [1], [5-8] to a symmetric and a public-key. In asymmetric cryptography, public key is used for encryption process and private key is used for decryption process. The prior is more important and secure than the later for cryptography, which depends on the length of the key used [4-9] and work of cryptography made during the computations.

From the survey works, motivated with the challenges in cryptography, a variation of DLPN with two order bits has been proposed, where the keys are dependent of LPN variables and is possible to enhance the scheme by odd and even bits with newly computed bits during the process of encryption and decryption [9-15]. Increased key generation time can be reduced by increasing the process of coding, it made a big-task in the implemented method, to provide security by the process, from attacks and made secure [16-28].

A. LPN

LPN [19] computational version is an analogue of linear codes decoding through random numbers, which is an NP-complete problem. The improvement in the efficiency is made through the sparse Fourier spectrum, that is LPN solver through $2^{O(n/\log n)}$ constant term with $\mu = O(1)$, is ≤ 0.5 & independent of secret size for all the values of n, is represented as n. Here $q = poly(n)$ is the number of training samples, with this the time complexity reaches to the training samples, for $q = O(n)$, and for $q = n + O(1)$ the time complexity goes to $2^{O(n^{1-e})}$; based on these, is the main drawback of the LPN, has to be reduced.

B. DLPN

In this, the public key becomes small, having a random public and private key vectors $a \in Z_2^n$ and $s \in Z_2^n$ respectively, based on these if an attacker gets $(a, \langle a, s\rangle + e)$, where $e \leftarrow Ber_\tau$, occurring only between $0 < \tau < 1$. But from the noise rate of LPN the distribution is $0 < \tau < 0.5$, through which attacker is able to differentiate the random $r \leftarrow Z_2$ and sampling $\langle a, r\rangle$ elements, which should be solved through DLPN [29], which is a public-key encryption scheme to improve the security.

A DLPN attacker with $(a, \langle a, s\rangle + e)$ set, where $e \leftarrow {Ber^{nxn}}_\tau$, remaining parameters at DLPN based. To distinguish between the random $r \leftarrow {Z^{nxn}}_2$ and sampling $\langle a, r\rangle$ elements, with a new sample $(a, \langle a, s\rangle + e)$, taking $\tau = O(1/\sqrt{n})$ noise rate and randomly selected public and private key vectors $a \in Z_2^{nxn}$ and $s \in Z_2^{nxn}$ respectively, by assuming the DLPN probabilistic polynomial time (PPT) parameters (n, τ) is negligible.

C. Contributions

The proposed work in this paper is an approach through the tradition public key cryptography scheme RSA [26-28] and current public key cryptography schemes LPN [29] and DLPN [29], so we restrict our discussions and contributions among RSA, LPN and DLPN only. This paper provides new constructions of encryption schemes from a variant of DLPN.

*Corresponding Authors

First contribution is to introduce a DLPN variety problem with $S \leftarrow Ber^{nxn}{}_{\tau}$ within the assumptions of normal DLPN problem. As a second contribution a key-bit is constructed into vector-bit through cryptographic operations. During the cryptographic decryption process, the n dimensional vector is having the hamming weight of n/2, with the plaintext-bit as even or odd or vice-versa. The probability order of odd and even plaintext-bits is monitored to decay their exponential exceeding expectations, through by reducing the error probability. In the third contribution, the odd and even plaintext-bits are ordered in a multi-bit level based on the encryption and decryption algorithm of the public key. Unlike the previous schemes, the proposed scheme is a minimization to the LPN and DLPN problem. Proposed authentication scheme is efficient as the surveyed schemes.

II. Related Works

A. Algorithms

Many schemes have been proposed for public key cryptography. In this paper, the contributions are on RSA algorithm, LPN and DLPN.

In RSA algorithm [22-25], it becomes difficult to find the decryption key under the large integer's factors. An enhanced RSA algorithm is proposed by factorizing and deriving the key variable and considering the third prime number by making the complexity more and robust. A new factor should be replaced to increase the complexity at cryptography process to reduce the track back difficulty in the product of three prime numbers, by achieving the increased time complexity.

In LPN [19],[29], the problems available are made in to two non-trivial solving methods, one is a type of method which intends for all possible noise vectors to be intended and the other which has a sub index time complexity $2^{O(n/\log n)}$. This complexity is increased further in to $2^{O(n/\log\log n)}$ with the sampling time of $n^{1+\varepsilon}$. A further improvement in the algorithm with less running time is to be made, and there is a need of polynomial time algorithms to solve the variety of LPN problems. So there is a need of a design for LPN based cryptographic applications, through symmetric encryption in public key scheme. Here a LPN based on public key encryption with the noise ratio of $\tau \approx 1/\sqrt{n}$ is considered. However, in all the variants of, an encoding error prevails which is a non-negligible. To solve these, in this paper, a matrix LPN problem is considered to solve the encoding error problem through Damgård's scheme.

In DLPN [29], the problem is to vary between the uniform distribution over the Z value and the number of samples given by the oracle LPN. It can be formulated by an optimization solution i.e., by using random matrix A with a random column vector c over Z, to find the vector v to maximise the equations of the scheme is Av=c. This illustrates a problem of decrypting a NP-hard, which is a random linear code. To solve these variants of LPN problems, require a sub-exponential query during the sub-exponential time. The DLPN is a variant of LPN_1 problem, with a distributed secret s is a uniform random variable and through Ber_{τ}^{k}. Here noise parameter made non-constant and it depends on the value of k, through a linear number of queries which are arbitrarily polynomial and matrix version of LPN_1. A public key cryptosystem based on LPN_1 is given as $\left|Pr_{s,A,e}\left[D(A, A \cdot s\Theta e) = 1 - Pr[D(A,r) = 1]\right]\right| \geq \epsilon$, where $A \leftarrow B_{\mu}^{q\times n}, s \leftarrow Z_2^n, e \leftarrow B_{\mu}^{q}\, and\, U_q$ is a uniform distribution over Z_2^q. The $LPN_{n,\mu,n+q}$ problem is hard and makes the problem of $Knapsack - LPN_{n,\mu,n+q}$ problem becomes hard. The DLPN problem is hard compare to LPN problem defined above, which leads to more complex results in public encryption key schemes, to make it available the design is made in black-box manner from the available DLPN problem identified, which is made for noise of $\mu = \omega(1)/\sqrt{n}$.

B. Mathematical Explanation

1) LPN: To make PKE correct, the PKE should be PKE= (KeyGen,Enc,Dec) for all the messages m ϵ M, the equation is given by: $Pr[Dec_{sk}(Enc_{pk}(m)) \neq m | (pk, sk) \leftarrow KeyGen(1^z)] \leq negl(z)$, where $negl(z)$ is negligible function. To discuss the LPN problem scenario, let us look in to the LPN oracle which is given by: $\{(v,b) | v \leftarrow Z_2^k, b =< v,s > \oplus\epsilon, \epsilon \leftarrow Ber_{\tau 0}\} \in Z_2^{k+1}$, where $s \leftarrow Z_2^k$, $\tau \in]0, \frac{1}{2}[$ is a constant noise parameter and $Ber_{\tau}$is the Bernoulli distribution with τ parameter. For the LPN search problem, depending on the distribution of As,τ the LPN oracle has the output independent random samples of $A_{s,\tau}^{LPN}$. Consider $LPN_{k,\tau}$as an instance of LPN with a secret key of size k and the noise parameter as τ. The algorithm which solves the $M(q,t,m,\theta)$ LPN search problem if $Pr\left[M^{A_{s,\tau}^{LPN}}(1^k) = s | s \leftarrow Z_2^k\right] \geq \theta$. It distinguishes between the distribution over the Z_2^{k+1} and the samples given by an LPN oracle. The search LPN problem is formulated as a optimization problem, through a random matrix A, a random column matrix b over Z_2, to find the vector s which maximises the number of equations of the system As=b.

2) DLPN: The decisional LPN problem is defined by the parameters $n \leftarrow N, \tau\, \epsilon\, R, \tau = \Theta(1/\sqrt{n})$ and randomly selected matrix $A \leftarrow Z_2^{n\times n}, S \leftarrow Z_2^{n\times n}$ as random selected matrix. The sample set of key can be obtained by the attacker in the form of (A,AS+E) by $E \leftarrow Ber_{\tau}^{n\times n}$, with the database sample (A,R), $R \leftarrow Z_2^{n\times n}$ having a non-negligible probability after getting the enough sample sets, which makes the DLPN problem to be solved. With the noise rate τ, the DLPN assumptions are defined with the probabilistic polynomial time (PPT) attacker including the parameter n which is negligible and is defined as $\tau = \Theta(1/\sqrt{n})$. The bit level encryption of DLPN is:

a) Choose $A \leftarrow Z_2^{n\times n}, S \leftarrow Ber_2^{n\times n}, E \leftarrow Ber_{\tau}^{n\times n}$, *compute* $B = AS + E$ *and* $KeyGen(1^n, \tau)$ *and returns a public key* $pk = (A, B)$ *and a private key* $sk = (S)$.

b) Choose encryption $Enc(pk, m)$, public key pk and user message $m\, \epsilon\, Z_2$, compute $c_1 = r^T A + e_1^T, c_2 = r^T B + e_2^T + mI$ and returns to a ciphertext $c = (c_1, c_2)$.

c) Choose decryption $Dec(sk, c)$, the private key sk and a ciphertext $c = (c_1, c_2)$, compute $d = c_1 \times S + c_2$ and returns m=0 for $h(d) \ll n/2$, and m=1 for $h(d) \gg n/2$.

To provide correctness of DLPN problem, define $X \sim Bin_{n,\tau}$ with an even variable with variations of $\frac{1}{2} + (1 - 2\tau^2)^2/2$, and define hamming weight of each column of odd variable with variations of $n(1-(1-2\tau^2)^n/2)$, with the selected scheme of $h(d) \ll n/2$ to meet its reduced decryption error.

III. Proposed Key Encryption Scheme

A. Proposed Scheme

Proposed scheme uses two prime messages in an order with the increased size. The message noise of these two orders generate the public key (P), a variable (O) and private key (Q). P and Q are generated with O parameter considered. Random messages Even() and Odd() are required to create the prime messages. It takes a time in generation of secure key using Even() and Odd() messages and find the noise in the message and time taken is also less by dividing them in to two categories, which makes the reduction in complexity of the algorithm. The value of O is generated in a random way and these values are transmitted through a sequence of newly generated that is, O_EO as a public key. It continues with the P and Q through the regenerative O and O_EO sequences, so it becomes difficult to the attackers to enter the system which is encrypted, which helps system to improve the security. Proposed key encryption scheme algorithm is described as follows.

B. Mathematical Representation of Proposed DLPN with two order bits Algorithm

It includes:

1) kO-DLPN of kO_KeyGen(1^n,τ) takes n as integer and τ as noise rate, by choosing a random matrix $A \leftarrow Z_2^{n\times n}, S \leftarrow Ber_\tau^{n\times n}, E \leftarrow Ber_\tau^{n\times n}$.

2) kO-DLPN of kO_Enc(pk, m) is divided in to two parts.

First is Even(), where m is converted to an even-square matrix $M^{Even} \in Z_2^{n\times n}$, if m_e=1, for M^{Even}e-th column of is 1 and similarly at each entry of the e-th column is 0, e.g., m=$(0,1,1,1)^T$, then $M^{Even} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, by choosing $E^{Even} \leftarrow Ber_\tau^{n\times n}$.

And second is Odd(), where m is converted to a odd-square matrix $M^{Odd} \in Z_2^{\overline{n\times n}}$, if m_e=0, each entry of the e-th column of M^{Odd} is 0 and similarly at each entry of the e-th column is 1, e.g., m=$(1,0,0,0)^T$, then $M^{Odd} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, by choosing $E^{Odd} \leftarrow Ber_\tau^{\overline{n\times n}}$.

3) kO-DLPN of kO_Dec(sk, c) with ciphertext $C = (C_{Even} \oplus C_1, C_2 \oplus C_{Odd})$.

C. Solution Equations for Proposed DLPN with two order bits Algorithm

It includes:

1) kO-DLPN of kO_KeyGen(1^n,τ): Compute $B = AS + E$, to return pk with key $sk = (S)$.

2) kO-DLPN of kO_Enc (pk, m) is divided in to two parts.

First is Even(), returns to ciphertext C=(C_{Even} and C_2) where the computations are C_{Even}=RA+E_{Even} and C_2=RB+E_2+M^{Even} with $E_{Even} \leftarrow Ber_\tau^{1\times n}$ and $E_2 \leftarrow Ber_\tau^{n\times n}$.

And second is Odd (), returns to ciphertext C=($C_1$and C_{Odd}) where the computations are C_1=RB+E_1+M^{Odd} and C_{Odd}=RA+E_{Odd} with $E_{Odd} \leftarrow Ber_\tau^n$ and $E_1 \leftarrow Ber_\tau^{n\times n}$.

3) kO-DLPN of kO_Dec(sk, c), returns $(C_1 \times C_{Even}) \times S + (C_2 \times C_{Odd})$.

IV. Application is a Web Model

Proposed scheme is applicable for secure data encryption and decryption to eliminate the noise words between the users. This scheme improves the security information transmission between multi-users utilizing web benefit as an admin middle person. It identifies the noise information in the users' message which is in encrypted unscrambled by user side and by admin encryption the noise words are recognized and identified.

Separate models are made - 1) A web-application (user and admin support) and 2) A web-server (server support). Web-application program encrypt user message received by admin through noisy message elimination during the decryption scheme and makes a web server benefit with noise-free message. The web-server receives the data processed from web applications, warns and removes user message information utilizing both sides of encryption and decryption. After admin information approval, web server restores the user message by eliminating the noise words and results the blocked user authentication for noise words presence and providing the message without any noise through the web application, which is illustrated in the below figures (Fig. 1 and 2).

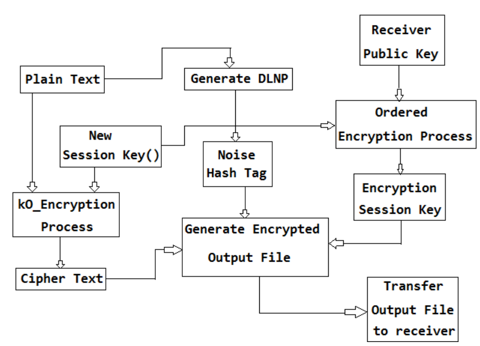

Fig. 1. Flowchart at the Sender Side.

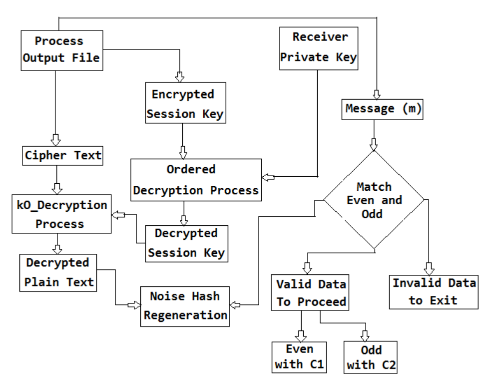

Fig. 2. Flow Chart at the Receiver Side.

V. Results and Discussions

The proposed scheme uses Client layer through HTML and CSS, Business layer through java and jdbc and Persistence through web server. All these three are integrated on Apache NetBeans platform. Here 128-bit security is used with n=29000 through 3072-bit security levels. This work is reviewed by other methods through the following parameters.

A. Key Generation Time

Table I list the comparison between proposed scheme with Damgård schemes [18] and PPKE based LPN [29] in computational efficiency.

All the above are with respective to LPN, the multiplications and additions have made the computational time to reduce. Proposed work is similar to PPKELPN but proposed work increases slightly in public key and ciphertext in both the scenarios and decryption error can be neglected. From Table II, the key generation time of proposed work is better than the reviewed works. From the experiments it is proved that proposed work key generation time is higher than RSA, Table II shows these results.

B. Encryption Time and Decryption Time

Comparing the performance of proposed work with PPKELPN , RSA(not padding) and Damgård's scheme, the proposed work illustrates better than RSA, Table III shows these results.

Comparatively the method proposed scheme is better than the surveyed works.

TABLE. I. Comparison between Proposed Work and Damgård Schemes and PPKE based LPN

Method	Public key size(bit)	Ciphertext size(bit)	Encoding error
Damgård for bit=1	$2n^2+2n$	n+1	Yes
PPKE based LPN for bit=1	$2n^2$	2n	No
Proposed for bit=1	n^2	N	No
Damgård's for bit=multi	$4n^2$	2n	Yes
PPKE based LPN for bit=multi	$2n^2$	$2n^2$	No
Proposed for bit=multi	$2n^2$	n^2+1	No

TABLE. II. Comparison between Proposed Work and RSA, ERSA, HRSA in Key Generation Time

Security level (128 bits)	Key generation time (ms)
RSA[24]	0.127
ERSA [27]	0.112
HRSA [28]	0.241
Proposed Work	0.352

TABLE. III. Comparison between Proposed Work and Reviewed in Encryption Time and Decryption Time

Security level (128 bits)	Encryption time(ms)	Decryption time (ms)
PPKE based LPN [29]	102.10	0.258
Damgård's scheme [18]	241.70	0.128
RSA(not padding) [12]	0.060	2.890
Proposed Work	99.85	0.119

VI. Conclusions

A cryptography scheme under public key through DLPN assumptions is an important research work, carrying many advantages comparatively. Due to decryption errors the existing systems are still having problems, which have to be corrected.

Through DLPN variant problem, a key-Ordered DLPN is proposed in this paper. There is a drastic change in the computing overhead of the proposed work compared to the PPKELPN, Damgård's scheme and RSA. Proposed work can withstand with the practical security like quantum attacks. A comparative result shows the proposed work gives high security.

VII. Future Scope

Further in future, through this work, design of public and private key cryptography to implement as a CCA level security, which can be made possible.

References

[1] X. Sun, B. Li, X. Lu, and F. Fang, ``CCA secure public key encryption scheme based on LWE without Gaussian sampling," in Proc. Int. Conf. Inf. Secur. Cryptol., vol. 9589, 2015, pp. 361378.

[2] Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, ``DivORAM: Towards a practical oblivious RAM with variable block size," Inf. Sci., vol. 447, pp. 111, Jun. 2018.

[3] C.-Z. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, ``Privacy-preserving Naive Bayes classiers secure against the substitution-then-comparison attack," Inf. Sci., vol. 444, pp. 7288, May 2018.

[4] P. Li et al., ``Multi-key privacy-preserving deep learning in cloud computing," Future Generat. Comput. Syst., vol. 74, pp. 7685, Sep. 2017.

[5] G. Liu, H. Li, and L. Yang, ``A topology preserving method of evolving contours based on sparsity constraint for object segmentation," IEEE Access, vol. 5, pp. 1997119982, 2017.

[6] N. Koblitz, A. Menezes, and S. Vanstone, ``The state of elliptic curve cryptography," Des., Codes Cryptogr., vol. 19, nos. 23, pp. 173193, 2000.

[7] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, ``Insight of the protection for data security under selective opening attacks," Inf. Sci., vols. 412413, pp. 223241, Oct. 2017.

[8] D. Boneh and A. Silverberg, ``Applications of multilinear forms to cryptography," J. Contemp. Math., vol. 324, no. 1, pp. 7190, 2003.

[9] J.-S. Coron, T. Lepoint, and M. Tibouchi, ``Practical multilinear maps over the integers," in Advances in CryptologyCRYPTO (Lecture Notes in Computer Science), vol. 8042. Berlin, Germany: Springer, 2013, pp. 476493.

[10] Y. Hu and H. Jia, ``Cryptanalysis of GGH map," Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Tech. Rep., Feb. 2016. [Online]. Available: http://eprint.iacr.org/2015/301.pdf

[11] C. Gentry, C. Peikert, and V. Vaikuntanathan, ``Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Annu. ACM Symp.Theory Comput., 2008, pp. 197206

[12] J. Li, Y. Li, X. Chen, P. Lee, and W. Lou, ``A hybrid cloud approach for secure authorized deduplication," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 12061216 May 2015.

[13] W. Chen, H. Lei, and K. Qi, ``Lattice-based linearly homomorphic signatures in the standard model," Theor. Comput. Sci., vol. 634, pp. 4754, Jun. 2016.

[14] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, ``Candidate indistinguishability obfuscation and functional encryption for all circuits," in Proc. Annu. IEEE Symp. Found. Comput. Sci., Oct. 2013, pp. 4049.

[15] A. Blum, A. Kalai, and H. Wasserman, ``Noise-tolerant learning, the parity problem, and the statistical query model," J. ACM, vol. 50, no. 4, pp. 506519, 2003.

[16] P. Kirchner, ``Improved generalized birthday attack," Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Tech. Rep., Jun. 2016. [Online].Available: http://eprint.iacr.org/2011/377.pdf

[17] A. Juels and A. Stephen, ``Authenticating pervasive devices with human protocols," in Proc. Annu. Int. Cryptol. Conf., vol. 3621, 2005, pp. 293308.

[18] J. Katz, J. S. Shin, and A. Smith, ``Parallel and concurrent security of the HB and HBC protocols," J. Cryptol., vol. 23, no. 3 pp. 402421, 2010.

[19] I. Damgård and S. Park, ``How practical is public-key encryption based on LPN and ring-LPN?" Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Tech. Rep., Jun. 2016. [Online]. Available: http://eprint.iacr.org /2012/699.pdf

[20] W. Stallings, "Cryptography and network security: principles and practice", sixth edition, 2014, ISBN: 0-13- 335469-5, pp. 9-60, 253-285.

[21] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM vol. 21 (2), pp.120–126, 1978.

[22] R S Dhakar, A K Gupta and P Sharma, "Modified RSA encryption algorithm (MREA)", 2nd ICACCT, IEEE, pp. 426-429, 2012.

[23] M.Thangavel, P. Varalakshmi, M. Murrali and K.Nithya, "An enhanced and secured RSA key generation scheme" Journal of Information Security and applications, Elsevier, vol 20, pp.3-10, 2015.

[24] F.Kong, J. Yu and L. Wu, "Security analysis of an RSA key generation algorithm with a large private key", Springer- Verlag Berlin Heidelberg, PP-95-101, 2011.

[25] L. H. Encinas, J. M. Masqu´e and A. Q. Dios, "An algorithm to obtain a RSA modulus with a large private key", Cryptology ePrint Archive: Report 2003/045.

[26] B.R. Ambedkar, A. Gupta,P. Gautam and S.S.Bedi, "An Efficient Method to Factorize the RSA Public Key Encryption." Communication Systems and Network Technologies (CSNT), 2011 International Conference on.

[27] R. Minni, K. Sultania and S.Mishra, "An algorithm to enhance security in RSA" , 4th ICCCNT, IEEE , pp.1-4, 2013.

[28] Jayraj Gondaliya at all.,Hybrid Security RSA Algorithm in Application of Web Service,2018 1st International Conference on Data Intelligence and Security, ©2018 IEEE, pp-149-152.

[29] Zhimin Yu at all.,A Practical Public Key Encryption Scheme Based on Learning Parity With Noise, Special Section On Information Security Solutions For Telemedicine Applications, IEEE Access, VOLUME 6, 2018, pp-31918-31923.