Proxy Re-Encryption using MLBC (Modified Lattice Based Cryptography)

Chandrakala B M[1]
Research Scholar,ISE DEPT,
Dayananda Sagar College of Engg ,Bengaluru,India
Chadrakala.pi@gmail.com

Dr.S C Linga Reddy[2]
Prof & Head,CSE DEPT,
Sri Venkateshwara College of engineering
sclingareddy@gmail.com

Abstract
In last few years, Proxy Re-Encryption has been used for forwarding the encrypted message to the user, these users are the one who has not been a part of encryption. In the past several scheme were developed in order to provide the efficient and secure proxy re-encryption. However, these methodology mainly focused on features like maximum key privacy, minimal trust proxy and others. In such cases the efficiency and security was mainly ignored. Hence, in order to provide the efficient and secure proxy re-encryption, we proposed an algorithm named as MLBC (Modified Lattice Based Cryptography) is proposed. Our method is based on the PKE (Public Key Encryption) and it provides more efficiency when compared to the other cryptography technique. Later in order to evaluate the algorithm simulation is done based on several parameter such as encryption time, proxy key generation time, Re-encryption time and Total computation time. Later, it is compared with the existing algorithm and the plotted graph clearly shows that our algorithm outperforms the existing algorithm.

Keywords: Proxy Re-Encryption, Security, MLBC, cryptography

Introduction
In recent years the data sharing as well as cloud storage have gained attention for serving the Customer-Oriented application namely iCloud [1], Google Drive [2], Microsoft SkyDrive[3], Dropbox[4] and others [5]. In cloud computing the user hires the computing storage space from CSP (Cloud Service Provider) in order to achieve the user requirement. Here, user uploads the file to the server and later, either they synchronize or download according to the requirement ,this in terms helps in providing flexibility. For example, any organization enables its employees to share and outsource the files in given public cloud [6]. Moreover, the employees of the same group can access the data shared by the organization at any instance of time, at any place and from any device. Primary benefits of sharing the data through the cloud is it is flexible along with this, the maintenance cost is much less and easily accessible [7].

In spite of being flexible and easily accessible group data sharing in the cloud has not been adopted by the different organization. This is due to the security concern. Security is said to be one of the main issue when it comes to sharing the data [8].since the data might have sensitive information that has to be accessed by only authorized user[9]. Hence, to get rid of the security issue, Encryption is introduced. Encryption is nothing but a kind of cryptographic technique that helps in encoding an information, which could only accessed by the authorized party not by unauthorized user. Moreover, it does not prevent interference, but it does denies for accessing the content [10].

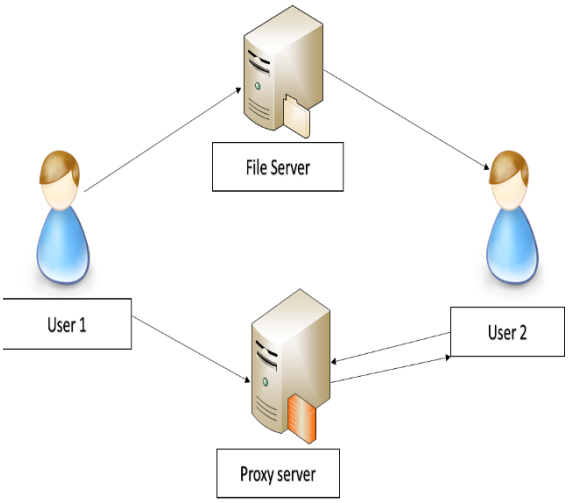

Figure 1 Typical Pre-Encryption

Proxy Re-Encryption methods are the cryptosystem that allows the proxies (Third parties) to change ciphertext that is encrypted from the one party such that it can be decrypted by the other [11] [12]. Typical proxy Re-encryption is shown in figure 1, here user1 has some sensitive data in encrypted form in given file server; user 2 tries to fetch the encrypted from given file server and later it transmits the files(encrypted) to the proxy. Now, Re-encryption key is sent by the user 1 to proxy, this in terms re-encrypts the files

978-1-5386-9482-4/19/$31.00 ©2019 IEEE

(encrypted) and sends the ciphertext(re-encrypted) and only the user 2 can decrypt from his given private key.

In general proxy re-encryption is applicable when the party consider it as A wants to disclose the message content that are sent to him and it is encrypted with the given public key to the defined third party let's say as B without disclosing the private key. A does not allow the proxy to read the message content. Hence A can designate a proxy in order to re-encrypt the message, which is send to B. This in term generate the new key so that B can use for decrypting the messages. Now, in case if A sends B message which was under A's key, the proxy tries to change the message. This scheme is applicable for the several purpose such as content distribution, law-enforcement monitoring and e-mail forwarding.

Proxy re-encryption is one of the novel data encryption method which is devised mainly for security and distributing the file. The main aim of proxy re-encryption is to allow the re-encryption of particular cipher text to the other given cipher text, it does not rely on the third party for transforming operation. Proxy re-encryption has gained a lot of interest in research are due to its capabilities of providing the security. Hence first [13] proposed proxy algorithm this allows the semi trusted proxy along with the re-encryption key knowledge for transforming the ciphertext into another ciphertext. However, the issue was that the proxy was not capable of obtaining the information about the PK (Private Keys) of delegate as well as delegator.[14] proposes a new technique namely IBC(Identity Based Conditional)-PRE is introduced in order to transform the ciphertexts subset to the other ciphertexts . This takes place from one identity to another identity. This model provides security in the RO (Random-oracle) scheme. However, these lacks with anonymity, which is essential in several applications.

[15] Proposed an attribute based PRE, this method was a semi-trusted proxy along with the extra information that can transform a cipher text in another cipher text; this is done under the set of attribute. This method allows the fine-grained control on the given encrypted data. ABE (Attribute Based Encryption) is said to be the generalized form of identity based Encryption. The two types are ciphertext and key policy. In [16] KP-ABE scheme is proposed, here encrypted one names each ciphertext with the descriptive attributes sets. In this each private key has an access scheme which mentions that which ciphertexts key can be used for decrypting.

In [16], C-PRE (Conditional-PRE) is proposed where ciphertext only satisfy the condition i.e. set by the one user and transformed by the proxy and decrypted by the user. Here, the efficient C-PRE scheme is proposed and this method comes under the BDF (Bilinear Diffe-Hellman) assumption. In quorum-based protocol, the proxy is parted into the several sub-components and these sub components controls the re-encryption key. IN this methodology the key are safe only until the proxies are honest. In [17] unidirectional proxy encryption is proposed. Here, the IBE scheme is applied by sharing the SK (Secret key) among the two given users. This scheme tries to solve the issue of proxy assigning.

[18] Proposed the first ABE (Attribute Based Encryption), here both secret key as well as ciphertext are labelled as the set of attributes. Here the user are able to decrypt the only available ciphertext when there exist a similarity between the decrypted one and the given ciphertext.

[19] proposed the scheme namely TR-PRE (Time-released), here the proxy ReEncrypt ciphertext along with the available release time under the given Public Key to another which was released under the same time by employing the RE-Encryption key which is provided by the given delegator.

Motivation and Contribution of research

Cloud Computing has become one of the eminent as well as hot topic from the industry as well as academia point of view. There are several advantage of cloud computing that includes the availability of various computing resources with ease as well as in cost effectively. However, the biggest challenge is to ensure the security of the data, this problem was reduced through the encrypting the data. Moreover, still there were many loopholes in security even after the introduction of proxy re-encryption. Hence to overcome this issue we have proposed MLBC(Modified- Lattice Based Cryptography) approach is proposed which is based on the public key encryption. Later, in order to prove the efficiency of algorithm we have implemented the proposed algorithm by varying the different key size and the result analysis clearly indicates that MLBC provides better efficiency than the other PK-cryptosystem(Public Key) along with that it also provides the better security since it is based on the Hard problems.

This research is organized in several section that follows as: The research background about the cloud and security is discussed in introduction part , later part of the same section discusses various existing methodology for proxy re-encryption. Followed by the existing system survey motivation and research contribution of the paper is discussed. In section2 the proposed methodology has been elaborated along with pictorial representation of proposed flow work, whereas section 3 deals with the result and comparative analysis which shows the performance evaluation of algorithm.. At last, section 4 concludes our paper.

Proposed Methodology

This section describes the motivation of MLBC (Modified Lattice Based Cryptography) technique. Several scheme has been proposed, which is discussed in the previous section. These schemes does provide the security, however, these methods either lacks with the security issue or lacks with

efficiency issue. Hence, in order to provide efficient as well as the secure proxy re-encryption, we proposed the MLBC (Modified Lattice Based Cryptography).

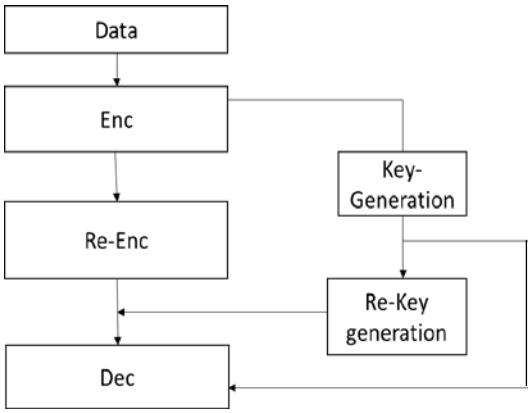

Figure 2 proposed methodology

The above figure depicts the proposed flow work and it also depicts the message flow, keys and cipher text. In the above figure PRE has two functions i.e. one that generates the key material and one that deals with messages and ciphertext. At first, Enc generates a ciphertext which encrypts the message whereas Dec deciphers the given ciphertext using the given SK (Secret Key). Re-Key generation tries to produce the key among the two user and ReEnc uses these key to transform the ciphertext.

At first, the MLBC (Modified Lattice based Cryptography) is introduced and the operation of the same is described. Later our method is extended for constructing the bidirectional multihop PRE (Proxy re-Encryption) method.

MLBC (Modified Lattice Based Cryptography)

MLBC is one of the PKE (Public Key Encryption) which is based on the Lattices. The main purpose of MLBC is to provide the efficiency and it is much better than the other PKC (Public Key Cryptosystem). MLBC is represented over the quotient ring

$$Q_{MLBC} = A[b]/(b^k - 1) \quad (1)$$

Here n represents the prime parameter Q_{MLBC} shows the integer polynomials that is comparatively less than the k.

MLBC (Modified Lattice Based Cryptography) Encryption

Proxy re-encryption technique namely MLBC is defined and it is PKE (Public Key Encryption) based scheme. The proposed algorithm is the extended version of the method that includes the re-encryption and re-encryption KG (Key Generation)-algorithm.

In here, the given private key $pvtk$ has the polynomial $p \in Q_{MLBC}$ that is selected randomly along with the coefficient, which is equivalent to 0,-1 and 1.

Encryption Process

MLBC (Modified Lattice Based Cryptography) Re-encryption

The MLBC Encryption has led to define the Re-Encryption known as MLBC Re-Encryption. The proposed method has four main process , these process are described below.

Generation of the Key: Outcome of this process is secret key as well as secret and public keys ($\text{seck}_Y, pubk_Y$). Here, at first the pair of polynomials is selected $(p_y, g_y) \in Q^2_{MLBC}$. The Private Key pvt_y is said to be the polynomial p_y, moreover the equation 2 shows the contents of the polynomial given in equation 2.

$$i_y = \text{m}.m.q_A.p_y^{-1} \; mod \; l \quad (2)$$

Generation of RE-Encryption key : when the secret key (input) $pvt_C = f_C$ and $pvt_y = p_y$, here the reencryption key is generated among the two users. This particular key is computed using the TPP (Three Party Protocol).

Encryption (pub_Y, D) : Here, after providing the input of public key $pubk_A$ and message $D \in Q_{MLBC/m}$, here the small random polynomial is generated by the encryption Enc . The output generated is ciphertext.

$$T_y = i_y{}^r + D \quad (3)$$

Re-Encryption process: Here the input given is ciphertext T_Y and the re-encryption key $RE_{Y \to C}$. The output generated after this process is ciphertext which is given in the below equation.

$$T_C = T_Y.RE_{Y \to C} + mn \quad (4)$$

Decryption Process: In this process, the input given is ciphertext T_A and secret key $Sec_Y = Y$. The output generated is given in equation 5

$$\text{D}=(T'_Y \; mod \; m) \quad (5)$$

Results and Analysis

This section of research shows the performance evaluation and comparative analysis of our re-encryption algorithm.

We have performed this particular research on windows 10 operating system loaded with i5 processor and 3.2 GHZ quad core. The system also has 8 GB of Ram and dedicated graphic of NVIDIA. Our algorithm is evaluated using the libraries of java cryptography in eclipse. Simulation is conducted by varying the key size such as (160-512, 160-1536, and 320-1536) for the various parameter such as encryption time, decryption time, re-encryption and total computation time. For each of this parameter the computation

time is noted and compared with the existing system as given below.

Comparative Analysis

In order to prove the benchmark of our algorithm against the existing system, we have compared the results based on several parameters.

In below figure, when the graph is observed we see that when the key size is (160-512) the computation time of the existing system is 0.015625 whereas in case of proposed system the computation time is 0.010416667. Similarly, when the key size is (160-1536), the computation time (in milliseconds) is 0.0625 whereas proposed system takes lesser time i.e. 0.041666667.In case of key size (320-1536) is 0.140625 whereas proposed system takes only 0.09375 ms to generate the proxy-key

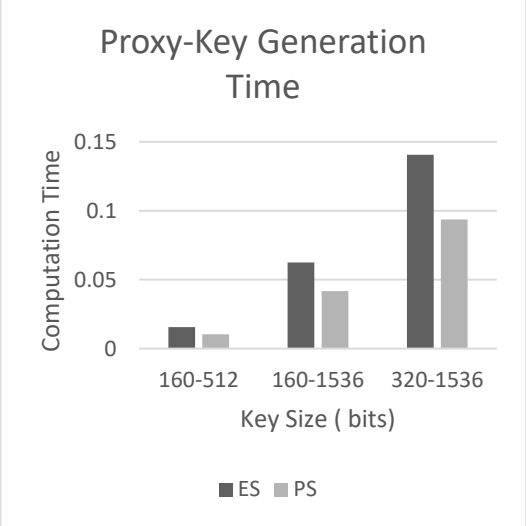

Figure 3 Proxy- Key Generation

Figure 4 presents the comparative analysis based on the Encryption time. In case of key size (160-512), the computation time is 0.015625 whereas proposed system takes 0.013020833 ms (milliseconds). In case of key size (160-5136) the encryption time taken is 0.015625 and proposed system take 0.013586957. For key size (320-1536), encryption time taken is 0.109375 and proposed system takes 0.093482906 ms (milliseconds)

Figure 5 shows the comparative analysis based on the Re-Encryption time. When simulation is performed on the varied key size, the proposed system performs much better than the existing system. In case of (160-512) key size, re-encryption time is 0.03125 ms whereas proposed system takes 0.00164647 ms for Re-encryption. Similarly, for (160-1536) key size existing system takes 0.03125 ms whereas proposed system takes 0.00163356 ms (milliseconds). For the key size (320-1536), existing system takes 0.109375 ms whereas 0.00495582 ms is taken by proposed system. The parameter analysis of Re-encryption shows that proposed system takes less time to re-encrypt.

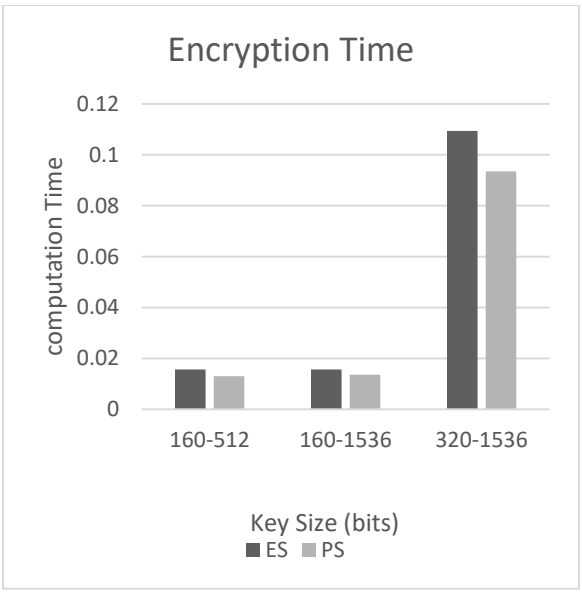

Figure 4 Encryption Time

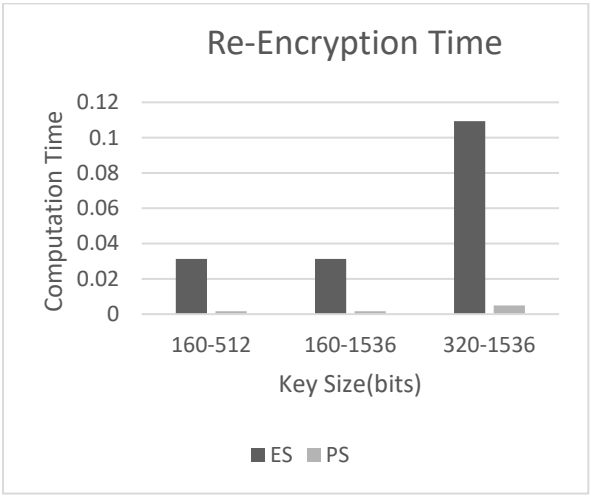

Figure 5 Re-Encryption Time

At last, the total computation time is computed and compared with the existing systems. In case of key size (160-512), the total time taken for computation is 0.53125 ms whereas proposed system takes 0.358866803. Similarly, for key size (160-1536) time taken by existing system is 1.109375 ms whereas proposed system 0.772634907 ms for (320-1536), time taken by existing system is 1.171875 ms and proposed system is 0.839221901.

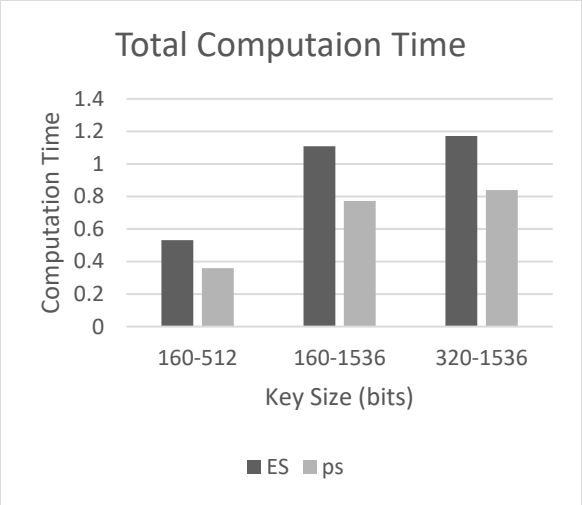

Figure 6 Total Computation Time

Conclusion

In this research work, we have proposed an algorithm namely MLBC (Modified based Lattice Cryptography) which is bidirectional and lattice based. Our algorithm is bidirectional; however, it is not collision-resistant. The prime goal to introduce this algorithm is to achieve high efficiency. Extensive simulation and result analysis shows that our scheme outperforms the existing algorithm. Although our algorithm provides a provable security and high efficiency. Still, there are several areas that we should look into such as consideration of Collision-resistance scheme. In future, our scheme can beconsidered for analyzing other Proxy Re-Encryption.

Reference

[1] https://www.icloud.com/

[2] https://www.google.com/drive/

[3] https://www.dropbox.com/

[4] https://onedrive.live.com/about/en-in/

[5] M. Sabbouh, K. McCracken and G. Cooney, "Data Sharing for Cloud Computing Platforms," *2014 IEEE International Congress on Big Data*, Anchorage, AK, 2014, pp. 621-628.

[6] https://en.wikipedia.org/wiki/Cloud_computing.

[7] E. Karafili, E. C. Lupu, A. Cullen, B. Williams, S. Arunkumar and S. Calo, "Improving data sharing in data rich environments," *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, 2017, pp. 2998-3005.

[8] N. Zhang, D. Liu and Y. Zhang, "A Research on Cloud Computing Security," *2013 International Conference on Information Technology and Applications*, Chengdu, 2013, pp. 370-373.

[9] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-based Key Agreement for Group Data Sharing in Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*.

[10] N. Jaber and Mohamad Fadli Bin Zolkipli, "Use of cryptography in cloud computing," *2013 IEEE International Conference on Control System, Computing and Engineering*, Mindeb, 2013, pp. 179-184.

[11] Z. Qin, H. Xiong, S. Wu and J. Batamuliza, "A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing," in *IEEE Transactions on Services Computing*.

[12] Hanshu Hong and Zhixin Sun, "Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search," *2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, 2017, pp. 218-223.

[13] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. Advances in Cryptology|EUROCRYPT'98, pages 127{144, 1998.

[14] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," in *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425-437, Feb. 2015.

[15] C. Fan, C. Wu, C. Chen, Y. Tseng and C. Feng, "Attribute-Based Proxy Re-encryption with Dynamic Membership," *2015 10th Asia Joint Conference on Information Security*, Kaohsiung, 2015, pp. 26-32.

[16]J. Shao, G. Wei, Y. Ling and M. Xie, "Identity-Based Conditional Proxy Re-Encryption," *2011 IEEE International Conference on Communications (ICC)*, Kyoto, 2011, pp. 1-5.

[17] B. Libert and D. Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption," in *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1786-1802, March 2011.

[18] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test in Cloud Computing," in *IEEE Access*, vol. 6, pp. 760-771, 2018.

[19] C. Fan, J. Chen, S. Huang, J. Huang and W. Chen, "Provably Secure Timed-Release Proxy Conditional Reencryption," in *IEEE Systems Journal*, vol. 11, no. 4, pp. 2291-2302, Dec. 2017.