Secure and Efficient Bi-Directional Proxy Re-Encryption Technique

Chandrakala B M.
Asst professor Dept. of ISE, Dayananda Sagar College of Engg, Bangalore, India
chadrakala.pi@gmail.com

Dr S.C.lingareddy
HOD Alpha College Of Engineering,Bangalore,India
sclingareddy@gmail.com

Abstract—Rapid development of communications over internet such as on-line money transaction, transaction of E-mail with sensitive data (medical data) and so on has led to need for strong cryptography technique. There has been continuous research going on to assure strong security by various cryptanalyst. However, performance, computation time and ease of use play a significant role in using the algorithm for implementation. Proxy re-encryption plays a significant role in protecting data that are stored in public environment (cloud). Many existing Proxy re-encryption technique induces high computation overhead due to adoption of public key cryptography such RSA (Rivet Shamir Adleman), ECC (Elliptical Curve Cryptography) etc. To address this work present a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique. Experiment is conducted for computation overhead by varying key and data size which attained significant performance improvement over existing Proxy Re-encryption scheme.

Keywords—Cryptography, Proxy Re-encryption, Data sharing, Security

I. INTRODUCTION

The wide availability low cost broadband/internet service has led to the growth of financial and business across various industries/organization. The growth of internet has led the organization to deliver customer services online such as social networking, online transaction, and customer service and so on. Internet has been integral part of every user as of today. Despite these benefit it still faces several issues and challenges such as integrity, confidentiality and privacy of data which is not trustable. To address this, cryptography mechanism has been adopted. Encryption and decryption is the integral part of cryptography mechanism. In Encryption the message are encoded by sender by applying some transformation technique and in decryption the message are decoded by receiver. The cryptograhic technique has been adopted in various domains such as cloud, social networking, Email service etc. when developing cryptography mechanism generating unbreakable cipher data is an art not technology. With the availability of high computing device and cloud technologies have led to development of strong cryptography mechanism which is the need of the hour.

Let consider a scenario that a person is on vacation and he is not able to access internet/mail. You would want the server to forward your encoded mail data to the receiver B who can decrypt the cipher data using his private key. A simple way is to store the private key in mail server. In that case when user receive the mail the server decode it using private key that is stored in server and re-encrypt message using B’s public key. Yet, such method is not desired solution, particularly for untrusted service provider [1] [2] [3], since the provider can obtain both your private key and actual data.

Proxy Re-Encryption [4] is an efficient strategy that assures sender secure storage and sharing of data/message on public storage environment and solves key management problems [4] [5]. Proxy Re-Encryption has been adopted by application domain ranging from encrypted email forwarding [6], vehicular ad hoc networks (VANETs) [7] [8] digital right management (DRM) [9] [10], distributed computing [11] [12], to group key management [13]. In Proxy Re-Encryption scheme a sender encode it file using public key and then store the cipher data on the semi-trusted server. When receiver request for data, the sender send the proxy key or re-encryption key associated with the intended receiver to the server as proxy. Then the receiver receives the re-encrypted cipher text then finally the receiver decrypt the cipher text with his private key to retrieve original data. The Proxy Re-Encryption technique generally assures security (1) that the proxy cannot re-encrypt the cipher data in a useful form before receiving the encryption key, and (2) that neither the receiver nor the server/proxy can obtain meaningful information of re-encrypted data.

The Proxy Re-Encryption is of two forms unidirectional and bi-directional. If re-encryption key $a^{a^{a^2}}$ inevitably permits the proxy to transform cipher data under $a^{a^2}$ into cipher data under $a^2$ then it is called as unidirectional. If re-encryption key $a^{a^2}$ inevitably permits the proxy to transform cipher data under $a^{a^2}$ into cipher data under $a^2$ and vice versa, then it is called as bidirectional. Any unidirectional scheme can be transformed into bidirectional but converse should hold. In [1] [3] presented a bilinear pairing unidirectional Proxy Re-Encryption to protect against CPA (Chosen Plaintext Attack). However it lacks security to protect attack against CCA (Chosen Cipher data Attack). To address this [14] presented CCA-secure bidirectional Proxy Re-Encryption technique. To address RCCA (Repayable Attack Chosen-Cipher data) security [15] presented a unidirectional Proxy Re-Encryption technique. Both these technique adopt bilinear pairing which requires high computation cost for modular exponentiation in finite fields [16] which adopts public key based cryptography mechanism.
To address this lattice based cryptography mechanism is adopted by various approaches. To resist the quantum attack, [17] presented the first lattice based Proxy Re-Encryption mechanism that realizes non-interactivity and collusion resilience. Further they presented, the security proof of their methodology is given in the selective model under the Learning with Error [18] assumption.

As in [18], [19] the Learning with Error assumption analytically has strong connection to lattice hardness assumptions, which are assumed safe in various factors. Though, there are possible “attacks” on Learning with Error, as in [20] [21] [22]. Therefore when designing a Learning with Error we need consider real world operation threat as in [20] among them Search-Learning with Error is most effective attack. In [23] presented unidirectional and multiple usage Proxy Re-Encryption technique by adopting multi-linear map [24] considering strong multi-linear groups and address the issues of [14] in designing Proxy Re-Encryption unidirectional and multihop.

This work presents a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique which is multihop (it supports multiple re-encryptions) which is presented in next section below.

The paper organization is as follows: In section two the proposed Bidirectional Proxy Re-encryption scheme is presented. Section three the experimental result are discussed. The last section paper is conclude with future work.

II. PROPOSED MODEL

This work present Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique. In lattice based cryptographic approach Java lattice based library is used which performs the mathematical operations of base level based cryptosystem. Let the Alice be person $X$ and bob be person $Y$. The proposed Bidirectional Proxy Re-Encryption scheme consists of following entities.

$\text{GenerateKey}()$: A pair of public and master key $(a_hX, m_hX)$ is the outcome of generate key function strategies for person $X$. By the use of $\text{GenerateKey}()$ a pair of public key and private key or master key generated. Public key is the $a_hX$ and master or private key is the $m_hX$ which is generated based on randomly selected polynomials.

If it randomly selects a polynomial pairs of $(hX, nX) \in F_q^2$, with fixed coefficient equivalent to $0, -1$ and the private polynomial $h$ has to be congruent to $1 \mod a$. Where $a$ the small polynomial. The public key consist of $a_hX$ that polynomial $tX = a \cdot nX \cdot hX^{-1} \mod b$ were the private key $hX$ is the polynomial $hX$.

$\text{RegenerateKey}(m_hX, m_hY)$. The input for re-encryption strategy is master key $m_hX = hX$ and $m_hY = hY$. The re-encryption key is computed among person $X$ and $Y$ as $pX \cdot X \cdot hX^{-1} \mod b$. The proxy key is computed where neither proxy nor $X, Y$ can obtain information about master key is as follows, Let $X$ choose an arbitrary $p \in F_q/b$ and transmit $p$ to proxy and $p \cdot hX \bmod b$ to $Y$. Similarly $Y$ transmits $p \cdot hX \cdot \frac{1}{hY} \bmod b$ to the proxy and then computation is done by proxy as $p \cdot hX \cdot \frac{1}{hY} \bmod b$.

$\text{Encrypt}(a_hX, D)$: On a given public key $a_hX$ and data $D \in F_q/b$ as input, the $\text{encrypt}$ function produces a ciphertext $T_x = tX \cdot m + D$ as and produces a trivial arbitrary polynomial $m \in F_q/b$ as output.

$\text{ReEncrypt}(pX \cdot X \cdot hX^{-1} \mod b)$: On a given ciphertext $T_x$ and re-encryption key $pX \cdot X \cdot hX^{-1} \mod b$ as input. The $\text{ReEncrypt}$ function generates ciphertext $T_y = T_x \cdot pX \cdot X \cdot hX^{-1} \mod b + aw$ and generates arbitrary polynomial $w \in F_q/b$ as output.

$\text{Decrypt}(m_hX, T_y)$: On a given ciphertext $T_y$ and master key $m_hX = hX$ as input. The $\text{Decrypt}$ function process $T_y = (T_y \cdot m + aw) \cdot hX^{-1} \mod b$ and produces the actual data $D = (T_y \cdot m + aw) \cdot hX^{-1} \mod b$ as output.

The Re-Encrypted cipher data form are represented as follows

$$T_x = (T_x \cdot pX \cdot X \cdot hX^{-1} \mod b + aw) \cdot hX^{-1} \mod b \quad (1)$$

$$= (anX^{-1} \cdot hX^{-1} \mod b + aw) \cdot hX^{-1} \mod b \quad (2)$$

When the re-encrypted cipher data is decrypted, the receiver multiplies the cipher data with its master key $hX$ as is follows

$$T_y \cdot T_x = (anX^{-1} \cdot hX^{-1} \mod b + aw) \cdot hX^{-1} \mod b \cdot hX \cdot hX^{-1} \mod b = anX \cdot m + aw \cdot hY + hX \cdot hX^{-1} \mod b \cdot hX \cdot hX^{-1} \mod b = anX \cdot m + aw \cdot hY + hX \cdot hX^{-1} \mod b \cdot hX \cdot hX^{-1} \mod b = D \quad (2)$$

The additional term is get ridden by obtaining mod $a$ and to obtain $hX \cdot hX^{-1} \mod b$ we required master key polynomial $hX$, therefore $(T_y \cdot hX) \cdot hX^{-1} \mod b = (anX \cdot m + aw \cdot hY + hX \cdot hX^{-1} \mod b) \cdot hX = D$, which is the actual data.

To prevent the simple cipher data only attack from the receiver we include the term $w$ in the process of re-encryption. Let consider that the cipher data form as $T_y = T_x \cdot pX \cdot X \cdot hX^{-1} \mod b$. The receiver could compute the master key of the sender based on criteria that $T_y \cdot hY = T_x \cdot hX$ is true, since $T_y = T_x \cdot pX \cdot X \cdot hX^{-1} \mod b$. Now let consider that $T_x$ is invertible mod $b$, the malicious/intruder can compute the master key by evaluating $hX = 1/T_x \cdot T_y \cdot hY$. Our models support multiple re-encryptions and it is bidirectional i.e. $pX \cdot X \cdot hX^{-1} \mod b$, the proxy can compute $pX \cdot X \cdot hX^{-1} \mod b = 1/(pX \cdot X \cdot hX^{-1} \mod b) = hX \cdot hY^{-1} \mod b$. This shows how the re-encryption keys are
computed \( p_{X-Y} = \frac{1}{m_{X-Y}} \), for bidirectional methodology.

The proposed Bidirectional Proxy Re-encryption scheme is evaluated and compared with existing Proxy Re-encryption scheme in terms of computation overhead for varied key size which is shown in below section.

III. EXPERIMENTAL RESULT AND ANALYSIS

The experiment is conducted on Windows 2007 enterprises operating system, I-5 3.2 Ghz quad core processor, CUDA NVIDIA 2GB dedicated graphic card, 8 GB Ram. The Proposed and Existing algorithm [25] is implemented by using java cryptography libraries in Eclipse Neon IDE (version 4.6). Simulation is conducted by varying key size and keeping the file size constant (1024 bytes) and the computation time are noted for Encryption, Re-encryption, Decryption and Total computation time (ms). The total computation is composed of the entire process including time taken to generate key.

In Fig. 1 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for encryption when key size is (256-1536) is 16.67%, for (256-4094) is 13.05% and for (320-4094) is 14.53% over Existing model. An average improvement of 14.75% is achieved by Proposed Model over Existing Model in terms of computation time for encryption.

In Fig. 2 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for re-encryption when key size is (256-1536) is 94.32%, for (256-4094) is 95.78% and for (320-4094) is 95.47% over Existing model. An average improvement of 94.001% is achieved by Proposed Model over Existing Model in terms of computation time for re-encryption.

In Fig. 3 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for decryption when key size is (256-1536) is 18.97%, for (256-4094) is 21.26% and for (320-4094) is 20.64% over Existing model. An average improvement of 20.208% is achieved by Proposed Model over Existing Model in terms of computation time for decryption.
Fig. 3. Computation time for Decryption for varied key size

In Fig. 4 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model when key size is (256-1536) is 53.42%, for (256-4094) is 52.02% and for (320-4094) is 53.03% over Existing model. An average improvement of 52.82% is achieved by Proposed Model over Existing Model in terms of total computation time.

IV. CONCLUSION

Providing security to data with least computation overhead is most desired. The existing technique adopts unidirectional based proxy re-encryption technique. To overcome the quantum security issue of public key cryptography many existing proxy re-encryption approaches have adopted lattice based cryptography mechanism which attained significant performance improvement but these techniques are unidirectional and induce decryption error for multiple re-encryption. Here we proposed a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique which is multipath. The proposed model achieves significant performance improvement interim of computation overhead over existing model. Simulation is conducted by vary key size an average improvement of 52.83% is achieved by proposed Proxy Re-encryption model over existing model in terms of computation overhead. In future we evaluate computation overhead of our model considering varied file size.

REFERENCES

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. ACM TISSEC, 9(1):1-30, Feb 2006.

[2] Tony Smith. DVD Jon: buy DRM-less Tracks from Apple iTunes March 18, 2005. Available at http://www.thereregister.co.uk/2005/03/18/itunes_pymusique.

[3] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. In NDSS, pages 29-43, 2005.

[4] M. Blaze, G. Bleumer and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,” Proc. Advances in Cryptology- EUROCRYPT ’98, Springer, Heidelberg, 1998, pp. 127-144.

[5] Matt Blaze and Martin Strauss. Atomic proxy cryptography. Technical report, AT&T Research, 1997.

[6] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Advances in Cryptology–EUROCRYPT’98. Springer, 1998, pp. 127–144.

[7] H. Xiong, Z. Chen, and F. Li, “Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy,” Security and Communication Networks, vol. 5, no. 12, pp. 1441–1451, 2012.

[8] T. Yang, H. Xiong, J. Hu, Y. Wang, W. Xin, Y. Deng, and Z. Chen, “A traceable privacy-preserving authentication protocol for VANETs based on proxy re-signature,” in 8th International Conference on Fuzzy Systems and Knowledge Discovery, vol. 4. IEEE, 2011, pp. 2217–2221.

[9] S. Lee, H. Park, and J. Kim, “A secure and mutualprofitabledrm interoperability scheme,” in Proceedings of IEEE Symposium on Computers and Communications. IEEE, 2010, pp. 75–80.

[10] G. Taban, A. A. C’ardenas, and V. D. Gligor, “Towards a secure and interoperable drm architecture,” in Proceedings of the ACM Workshop on Digital Rights Management. ACM, 2006, pp. 69–78.

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proceedings of the 2005 Symposium on Network and Distributed System Security, 2005.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Transactions on Information and System Security (TISSEC’06), vol. 9, no. 1, pp. 1–30, 2006.

[13] Y.-R. Chen, J. Tygar, and W.-G. Tseng, “Secure group key management using uni-directional proxy re-encryption schemes,” in IEEE
International Conference on Computer Communications. IEEE, 2011, pp. 1952–1960.

[14] R. Canetti and S. Hohenberger, “Chosen-ciphertext secure proxy re-encryption,” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 185–194.

[15] B. Libert and D. Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. In Proc. of PKC’08, LNCS 4929, pp. 360-379, Springer-Verlag, 2008.

[16] J. Baek, R. Safavi-Naini, and W. Susilo. Certificateless Public Key Encryption without Pairing. In Proc. of ISC’05. LNCS 3650, pp. 134-148, Springer-Verlag, 2005.

[17] E. Kirshanova. “Proxy re-encryption from lattices,” in Public Key Cryptography–PKC’14. Springer, 2014, pp. 77–94.

[18] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) STOC, pp. 84–93. ACM (2005).

[19] Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stuht’z, D.: Classical hardness of learning with errors. In: Bonh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC, pp. 575–584. ACM (2013).

[20] Rekert, M., Schneider, M.: Estimating the security of lattice-based cryptosystems. Cryptology ePrint Archive, Report 2010/137 (2010), http://eprint.iacr.org/.

[21] Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography, pp. 147–191. Springer, Heidelberg (2009).

[22] Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Kiyasu, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (2011).

[23] T. Fei, L. Hongda, and J. Chang, “Multi-hop unidirectional proxy re-encryption from multilinear maps,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 98, no. 2, pp. 762–766, 2015.

[24] S. Garg, C. Gentry, and S. Halevi, “Candidate multilinear maps from ideal lattices.” in Advances in Cryptology–Eurocrypt’13, vol. 7881. Springer, 2013, pp. 1–17.

[25] Aono, Y., Boyen, X., Phong, L.T., Wang, L.: Key-private proxy re-encryption under LWE. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT, vol. 8250, pp. 1–18. Springer, Heidelberg, 2013.