The Development of Proxy Re-Encryption

Yepeng Liu[1, 2], Yongjun Ren[1, 2, *], Qirun Wang[3] and Jinyue Xia[4]

Abstract: With the diversification of electronic devices, cloud-based services have become the link between different devices. As a cryptosystem with secure conversion function, proxy re-encryption enables secure sharing of data in a cloud environment. Proxy re-encryption is a public key encryption system with ciphertext security conversion function. A semi-trusted agent plays the role of ciphertext conversion, which can convert the user ciphertext into the same plaintext encrypted by the principal's public key. Proxy re-encryption has been a hotspot in the field of information security since it was proposed by Blaze et al. [Blaze, Bleumer and Strauss (1998)]. After 20 years of development, proxy re-encryption has evolved into many forms been widely used. This paper elaborates on the definition, characteristics and development status of proxy re-encryption, and classifies proxy re-encryption from the perspectives of user identity, conversion condition, conversion hop count and conversion direction. The aspects of the existing program were compared and briefly reviewed from the aspects of features, performance, and security. Finally, this paper looks forward to the possible development direction of proxy re-encryption in the future.

Keywords: Proxy re-encryption, bilinear pairing, information security.

1 Introduction

Cloud services make it easy to synchronize files between different devices or to provide computing and storage resources to remote users [Liu, Peng and Wang (2018)]. With the increasing variety of cyber-attacks [Zhang, Yang, Zhong et al. (2018)], people are paying increasing attention to the security of personal data on cloud servers. Users usually encrypt the uploaded data in case lose control of their data by passing the plaintext to a semi-trusted cloud provider. However, if Alice wants to share the encrypted data with Bob, it will face the embarrassing situation that Bob cannot decrypt the data. Unless Alice gives her private key to Bob, it is not feasible. One way to cope is that Alice

[1] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

[2] Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, Nanjing, China.

[3] School of Engineering and Technology, University of Hertfordshire, Hertford, UK.

[4] International Business Machines Corporation (IBM), New York, USA.

[*] Corresponding Author: Yongjun Ren. Email: renyj100@126.com

downloads the data locally for decryption and then sends the plaintext to Bob. However, this will consume Alice's massive amount of time, computing resources and communication resources, and cloud services will become meaningless. This example shows that the traditional public key cryptography solution cannot solve the problem of data security sharing in the cloud service environment.

Proxy re-encryption, a cryptosystem with security conversion, is very suitable for this situation. In the PRE-system, a semi-trusted proxy plays the role of ciphertext conversion, which can directly convert Alice's ciphertext into a re-encrypted ciphertext that can be decrypted by Bob's private key. The classic proxy re-encryption model is shown in Fig. 1. While the agent is unable to obtain any valuable information in this process, proxy re-encryption is a hotspot in the field of cryptography and information security. It has a large number of research results and has been widely used in different fields.

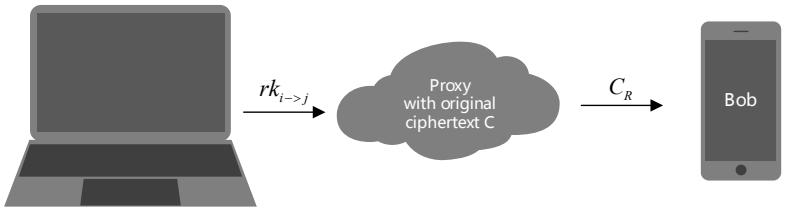

Figure 1: Classic proxy re-encryption scheme

In the first chapter, the basic concept of proxy re-encryption is expounded. In the second chapter, the scheme of proxy re-encryption is classified. The third chapter shares some research history and research status of proxy re-encryption. The fourth chapter illustrates some practical applications of proxy re-encryption. Finally, the future research direction of proxy re-encryption is prospected.

The abbreviations appearing in this article are listed in Tab. 1.

Table 1: Abbreviations in this paper

Abbreviation	Full name
CCA	Chosen-Ciphertext Attack
CCA2	Adaptive Chosen-Ciphertext Attack
CPA	Chosen-Plaintext Attack
C-PRE	Conditional Proxy Re-Encryption
DDH	Decisional Diffie-Hellman
H-PRE	Homomorphic Proxy Re-Encryption Scheme
K-PRE	Key-private Proxy Re-Encryption
LWE	Learning with Errors
PBRE	Proxy Broadcast Re-Encryption
RCCA	Repayable Chosen-Ciphertext Attack

2 The classification of PRE

There are several ways to classify proxy re-encryption:

1. According to the ciphertext conversion direction, it can be divided into one-way proxy re-encryption or two-way proxy re-encryption. The former can only convert Alice's ciphertext into Bob's ciphertext. The latter can not only realize one-way functions but also convert Bob's ciphertext into Alice's ciphertext again.
2. According to the ciphertext conversion times, it can be divided into single-hop proxy re-encryption or multi-hop proxy re-encryption. The former can only re-encrypt Alice's ciphertext once; the latter can re-encrypt the re-encrypted ciphertext again.
3. According to the user identification method, it can be divided into public key-based proxy re-encryption and identity-based proxy re-encryption. The former uses a string of random numbers that have no practical meaning to identify users and relies on trusted third to perform user public key queries. The latter uses the identity of the signer as the public key for verification.
4. According to whether there are conversion conditions, it can be divided into unconditional proxy re-encryption and conditional proxy re-encryption. In the unconditional proxy scheme, if Alice sends the translation key to the proxy, the proxy can arbitrarily convert any ciphertext that Alice stores in the proxy. In conditional proxy re-encryption, the proxy performs a re-encryption operation on the ciphertext that meets the conditions set by Alice and effectively controls the conversion transformation permission of the proxy, wherein the transition conditions are further divided into fuzzy conditions, fine-grained conditions, and so on.
5. According to whether the agent can convert ciphertext to multiple users at one time, it can be divided into one-to-one proxy re-encryption and broadcast proxy re-encryption. If Alice wants to share encrypted files with multiple users, the proxy must perform multiple re-encryption operations in one-to-one proxy re-encryption. In the broadcast proxy re-encryption, the proxy only needs to perform a re-encryption operation once, and Alice's re-encrypted ciphertext can be decrypted by Bob, Carol, Dave, and others.
6. According to the mathematical tools used in the construction of the proxy re-encryption scheme, it can be divided into proxy re-encryption based on bilinear pairing, proxy re-encryption based on multi-linear pairing, proxy re-encryption based on LWE, and so on. Compared with other mathematical tools, LWE-based solutions can theoretically be anti-quantum computer cracking.
7. In the security proof, the security of proxy re-encryption can be proved under a random oracle model or standard model. The random oracle model is usually an idealized substitute for the hash function in reality. The scheme that proves the security under the random oracle model is not necessarily safe in the actual implementation. The standard model does not rely on the random oracle model, so it has more application value. According to security, the security level of the proxy re-encryption scheme can be classified into CPA security or CCA security.
8. Some schemes also have some unique properties, such as anti-collusion attacks, keyword search, homomorphic encryption, and so on. Taking the anti-collusion attack as an example. In the proxy re-encryption scheme, there may be a case where the proxy

collaborates with Bob to obtain Alice's private key or another ciphertext, and the scheme against the collusion attack can effectively prevent such a situation from occurring.

3 The evolution of PRE

Blaze et al. [Blaze, Bleumer and Strauss (1998)] first proposed the concept of proxy re-encryption in 1998, and constructed a two-way, multi-hop proxy re-encryption scheme based on the ElGamal algorithm [ElGamal (1985)]. In the paper, Blaze proves that the scheme is CPA safe under the assumption of DDH difficulties. Blaze left an open question: how to construct a one-way proxy re-encryption scheme. However, in this scheme, the proxy and the re-encrypted ciphertext recipient (Bob) can collude to obtain the private key of the original ciphertext owner (Alice), and cannot resist collusion attacks.

In 1999, Jahobsson [Jakobsson (1999)] proposed an arbitration-based PRE scheme. He divided the agent into several sub-agents, each of which controlled a part of the proxy re-encryption key so that as long as some of the agents were honest, the security of Alice's private key could be guaranteed. The program partially solved the problem of collusion attacks.

In 2003, Ivan [Ivan (2003)] first gave a general method for constructing a one-way proxy re-encryption scheme based on the key sharing mechanism. Ivan splits the user's private key into two, one for the agent and the other for the re-encrypted ciphertext recipient. Although the solution solves the problem that the proxy distributes the decryption authorization independently, it cannot achieve key optimization and anti-collusion attacks.

In 2005, Ateniese first formalized the proxy re-encryption and its security model, and for the first time used a bilinear pair to construct a one-way proxy re-encryption scheme. The solution implements master key security and is resistant to collusion attacks. The author then introduced time slices based on the scheme to satisfy the transient [Ateniese (2006)]. However, this solution can only achieve CPA security and cannot meet the needs of practical applications. The author then proposes an open question on how to construct a CCA security proxy re-encryption scheme.

In 2007, Canetti et al. [Canetti and Hohenberger (2007)] first proposed a bidirectional multiplexing proxy re-encryption scheme that satisfies CCA security and proved that the scheme is semantically secure under the standard model and solves the above openness problem. However, this paper proposes more open questions about how to construct a proxy re-encryption scheme that does not rely on bilinear pairing and CCA security. In the same year, Green et al. [Green and Ateniese (2007)] proposed the identity-based proxy re-encryption scheme for the first time and constructed a CCA security scheme based on Boneh-Franklin.

In 2008, Libert et al. [Libert and Vergnaud (2008)] proposed the first one-way proxy re-encryption scheme that demonstrates RCCA security under the standard model. In the same year, Deng et al. [Deng, Weng, Liu et al. (2008)] constructed a bidirectional proxy re-encryption scheme which is independent of bilinear pairs and CCA security and solved Canetti's openness problem. However, this solution is not non-interactive and non-transitive and cannot resist collusive attacks.

In 2009, Shao et al. [Shao and Cao (2009)] constructed the first one-way proxy re-encryption scheme without bilinear and CCA security at the PKC conference. Weng et al. [Weng, Deng, Ding et al. (2009)] first proposed the concept of conditional proxy re-encryption and constructed a CCA-secured C-PRE scheme. Only when the ciphertext satisfies the conditions set by Alice, the proxy can convert the ciphertext into Bob's ciphertext. Therefore, conditional proxy re-encryption can effectively control the authority of the proxy to convert Alice ciphertext. Ateniese et al. [Ateniese, Benson and Hohenberger (2009)] proposed the concept of key privacy proxy re-encryption (K-PRE) at CT-RSA 2009 and constructed a CPA security scheme. In this scenario, the proxy cannot obtain information about Alice or Bob even if it has a re-encryption key. Chu et al. [Chu, Weng, Chow et al. (2009)] proposed the first conditional proxy broadcast re-encryption. In the previous scenario, if Alice wanted to share her ciphertext to multiple users, the proxy needed to re-encrypt each user individually. In the BPRE scheme, the ciphertext produced by the proxy for re-encryption operation can be directly decrypted by multiple users within a group.

In 2010, Sur et al. [Sur, Jung, Park et al. (2010)] proposed the concept of certificateless-based proxy re-encryption (CL-PRE) and constructed a scheme. Matsuda et al. [Matsuda, Nishimaki, Tanaka et al. (2010)] construct a bidirectional multiplexing proxy re-encryption scheme without a bilinear pairing through the lossy trapdoor function. Yau et al. [Yau, Phan, Heng et al. (2010); Shao, Cao, Liang et al. (2010)] proposed proxy re-encryption with keyword research (PRES).

In 2013, Aono et al. [Aono, Boyen and Wang (2013)] first constructed a K-PRE scheme based on LWE under the standard model. LWE is a standard hard problem on Lattices that can cope with the threat of quantum computers. Isshiki et al. [Isshiki, Nguyen and Tanaka (2013)] extended the security definition of proxy re-encryption and proposed a more secure CCA security model.

In 2014, Kirshanova [Kirshanova (2014)] proposed a unidirectional proxy re-encryption scheme based on the LWE difficult problem and gave the CCA security certificate.

In 2015, Liang et al. [Liang, Au, Liu et al. (2015)] propose a new ciphertext-policy attribute-based proxy re-encryption scheme. This scheme is proved adaptively chosen ciphertext secure and reduces the computation and communication costs of re-encryption key generation and re-encryption.

In 2017, Bellafqira et al. [Bellafqira, Coatrieux, Bouslimi et al. (2017)] proposed a homomorphic one-way anti-collusive attack proxy re-encryption scheme. This technique allows for retrieval, comparison, and other operations in encrypted data without the need to decrypt the data while getting the right results. The significance is to fundamentally solve the confidentiality problem when delegating data and its operations to third parties.

In 2018, Wang et al. [Wang, Xhafa, Ma et al. (2018)] first proposed the concept of PRE+ and constructed a specific scheme. This scheme passes the operation of generating the re-encryption key to the encryptor by the principal. PRE+ can implement fine-grained delegation and non-transferable attributes based on the message level. Tang et al. [Tang, Lian and Zhao (2018)] proposed a new proxy re-encryption with keyword search scheme. The improved solution does not need to re-encrypt the file ciphertext as in the conventional scheme, but re-encrypts the ciphertext of keywords corresponding to the file.

4 The application of PRE

The file sharing system is the most typical application of proxy re-encryption. Ge et al. [Ge, Susilo, Fang et al. (2018)] proposed a key-policy attribute-based proxy re-encryption and applied it to a data sharing system like Dropbox. Luo et al. [Luo and Ma (2018)] proposed an identity-based proxy re-encryption system and applied it to cloud storage. In this system, Alice can withdraw the re-encrypted ciphertext that the proxy has converted.

In addition, the variant of proxy re-encryption has a broader range of applications. Xu et al. [Xu, Jiao, Wu et al. (2016)] proposed a fine-grained broadcast proxy re-encryption scheme and applied it to the email system. Vijayakumar et al. [Vijayakumar, Priyan, Ushadevi et al. (2018)] proposes a searchable proxy re-encryption scheme and uses it in the E-Health Cloud. Polyakov et al. [Polyakov, Rohloff, Sahu et al. (2017)] proposed a secure multi-hop one-way proxy re-encryption scheme based on Ring-LWE and applied it to Publish/Subscribe Systems. Manzoor et al. [Manzoor, Liyanage, Braeken et al. (2018)] proposed a blockchain-based proxy re-encryption scheme, built an innovative sensor data storage platform and applied it to IoT Data Sharing.

5 Conclusion

After more than 20 years of development, proxy re-encryption has evolved into many forms and is widely used. However, with the rapid change of quantum computers, RSA-based cryptographic algorithms face unprecedented challenges. LWE can reduce the proxy re-encryption to the difficult problem of the grid and obtain the anti-quantum computer characteristics. However, the LWE-based proxy re-encryption scheme is still in its infancy, and schemes types are far less than those based on bilinear pairs. It is foreseeable that anti-quantum computer proxy re-encryption will become a new research hotspot in the future.

Acknowledgment: This work is supported by the NSFC (Nos. 61772280, 61702236), the Changzhou Sci & Tech Program (No. CJ20179027), and the PAPD fund from NUIST. Prof. Yongjun Ren is the corresponding author.

References

Aono, Y.; Boyen, X.; Wang, L. (2013): Key-private proxy re-encryption under LWE. *International Conference on Cryptology in India*, pp. 1-18.

Ateniese, G.; Fu, K.; Green, M.; Hohenberger, S. (2006): Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information System Security*, vol. 9, no. 1, pp. 1-30.

Ateniese, G.; Benson, K.; Hohenberger, S. (2009): Key-private proxy re-encryption. *Topics in Cryptology-CT-RSA 2009*, pp. 279-294.

Bellafqira, R.; Coatrieux, G.; Bouslimi, D.; Quellec, G.; Cozic, M. (2017): Proxy Re-encryption based on homomorphic encryption. *Proceedings of the 33rd Annual Computer Security Applications Conference*, pp. 154-161.

Blaze, M.; Bleumer, G.; Strauss, M. (1998): Divertible protocols and atomic proxy

cryptography. *Advances in Cryptology-EUROCRYPT'98*, pp. 127-144.

Canetti, R.; Hohenberger, S. (2007): Chosen-ciphertext secure proxy re-encryption. *Proceedings of the 14th ACM conference on Computer and Communications Security*, pp. 185-194.

Chu, C. K.; Weng, J.; Chow, S. S.; Zhou, J.; Deng, R. H. (2009): Conditional proxy broadcast re-encryption. *Australasian Conference on Information Security and Privacy*, pp. 327-342.

Deng, R. H.; Weng, J.; Liu, S.; Chen, K. (2008): Chosen-ciphertext secure proxy re-encryption without pairings. *Cryptology and Network Security*, pp. 1-17.

Dodis, Y. (2003): Proxy cryptography revisited. *Proceedings of 10th Annual Network and Distributed System Security Symposium-NDSS'03*.

ElGamal, T. (1985): A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469-472.

Ge, C.; Susilo, W.; Fang, L.; Wang, J.; Shi, Y. (2018): A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. *Designs, Codes and Cryptography*, vol. 86, no. 11, pp. 2587-2603.

Green, M.; Ateniese, G. (2007): Identity-based proxy re-encryption. *Applied Cryptography and Network Security*, pp. 288-306.

Isshiki, T.; Nguyen, M. H.; Tanaka, K. (2013): Proxy re-encryption in a stronger security model extended from CT-RSA2012. *Cryptographers' Track at the RSA Conference*, pp. 277-292.

Jakobsson, M. (1999): On quorum controlled asymmetric proxy re-encryption. *Public Key Cryptography*, pp. 112-121.

Kirshanova, E. (2014): Proxy Re-encryption from Lattices. *Public-Key Cryptography-PKC 2014*, pp. 77-94.

Liang, K.; Au, M. H.; Liu, J. K.; Susilo, W.; Wong, D. S. et al. (2015): A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. *Future Generation Computer Systems*, vol. 52, pp. 95-108.

Libert, B.; Vergnaud, D. (2008): Unidirectional chosen-ciphertext secure proxy re-encryption. *Public Key Cryptography-PKC 2008*, pp. 360-379.

Liu, Y.; Peng, H.; Wang, J. (2018): Verifiable diversity ranking search over encrypted outsourced data. *Computers Materials & Continua*, vol. 55, no. 1, pp. 37.

Luo, W.; Ma, W. (2018): A secure revocable identity-based proxy re-encryption scheme for cloud storage. *Cloud Computing and Security*, pp. 519-530.

Matsuda, T.; Nishimaki, R.; Tanaka, K. (2010): CCA proxy re-encryption without bilinear maps in the standard model. *Public Key Cryptography-PKC 2010*, pp. 261-278.

Manzoor, A.; Liyanage, M.; Braeken, A.; Kanhere, S. S.; Ylianttila, M. (2018): Blockchain based proxy re-encryption scheme for secure IoT data sharing. arXiv preprint arXiv:.02276.

Polyakov, Y.; Rohloff, K.; Sahu, G.; Vaikuntanathan, V. (2017): Fast proxy re-encryption for publish/subscribe systems. *ACM Transactions on Privacy and Security*,

vol. 20, no. 4, pp. 1-31.

Shao, J.; Cao, Z. (2009): CCA-secure proxy re-encryption without pairings. *Public Key Cryptography*, pp. 357-376.

Shao, J.; Cao, Z.; Liang, X.; Lin, H. (2010): Proxy re-encryption with keyword search. *Information Sciences*, vol. 180, no. 13, pp. 2576-2587.

Sur, C.; Jung, C. D.; Park, Y.; Rhee, K. H. (2010): Chosen-ciphertext secure certificateless proxy re-encryption. *Communications and Multimedia Security*, pp. 214-232.

Tang, Y.; Lian, H.; Zhao, Z.; Yan, X. (2018): A proxy re-encryption with keyword search scheme in cloud computing. *Computers Materials & Continua*, vol. 56, no. 2, pp. 339-352.

Vijayakumar, V.; Priyan, M. K.; Ushadevi, G.; Varatharajan, R.; Manogaran, G. et al. (2018): E-health cloud security using timing enabled proxy re-encryption. *Mobile Networks and Applications*, pp. 1-12.

Wang, X. A.; Xhafa, F.; Ma, J.; Barolli, L.; Ge, Y. et al. (2018): PRE+: dual of proxy re-encryption for secure cloud data sharing service. *International Journal of Web*, vol. 14, no. 1, pp. 44-69.

Weng, J.; Chen, M.; Yang, Y.; Deng, R.; Chen, K. et. al (2010): CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles. *Science China Information Sciences*, vol. 53, no. 3, pp. 593-606.

Xu, P.; Jiao, T.; Wu, Q.; Wang, W.; Jin, H. (2016): Conditional identity-based broadcast proxy re-encryption and its application to cloud email. *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-79.

Yau, W. C.; Phan, R. C. W.; Heng, S. H.; Goi, B. M. (2010): Proxy re-encryption with keyword search: new definitions and algorithms. *Security Technology, Disaster Recovery and Business Continuity*, pp. 149-160.

Zhang, S.; Yang, X.; Zhong, W.; Sun, Y. (2018): A highly effective dpa attack method based on genetic algorithm. *Computers Materials & Continua*, vol. 56, no. 2, pp. 325-338.