Wang, X.A. [et al.] (2016) Identity based proxy re-encryption scheme (IBPRE+) for secure cloud data sharing. *2016 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2016, 7-9 September 2016, Ostrava, Czech Republic: proceedings*. [S.l.]: IEEE, 2016. Pp. 44-48. Doi: http://dx.doi.org/10.1109/INCoS.2016.83.

Identity Based Proxy Re-encryption Scheme (IBPRE$^+$) for Secure Cloud Data Sharing

Xu An Wang[1,2], Fatos Xhafa[3], Zhiheng Zheng[1], Jinting Nie[1]
[1]Engineering University of Chinese Armed Police Force, P. R. China
[2]School of Cyber Engineering, Xidian University, P. R. China
[3]Department of Computer Science, Technical University of Catalonia, Spain
wangxazjd@163.com, fatos@cs.upc.edu

***Abstract*— In proxy re-encryption (PRE), a proxy with re-encryption keys can transfer a ciphertext computed under Alice's public key into a new one, which can be decrypted by Bob only with his secret key. Recently, Wang *et al*. introduced the concept of PRE plus (PRE$^+$) scheme, which can be seen as the dual of PRE, and is almost the same as PRE scheme except that the re-encryption keys are generated by the encrypter. Compared to PRE, PRE$^+$ scheme can easily achieve this important property: the message-level based fine-grained delegation. In this paper, we extend the concept of PRE$^+$ to the identity based setting. We propose a concrete IBPRE$^+$ scheme based on 3-linear map and roughly discuss its properties. We also demonstrate potential application of this new primitive to secure cloud data sharing.**

I. Introduction

In 1998, Blaze, Bleumer and Strauss [1] proposed the concept of proxy re-encryption (PRE), where a semi-trusted proxy can transform a ciphertext for Alice into another ciphertext that Bob can decrypt. However, the proxy can learn nothing about the corresponding plaintext. According to the direction of transformation, PRE schemes can be classified into two types, namely, bi-directional or uni-directional. A PRE scheme is called bidirectional if the proxy can use the re-encryption key to divert ciphertexts from Alice to Bob and vice-versa. Otherwise, it is called unidirectional. In unidirectional PRE schemes, the proxy can only transform in one direction. Blaze *et al*. [1] also gave another method to classify PRE schemes, called multi-use, i.e., the ciphertext can be transformed from Alice to Bob to Charlie and so on; and single-use, i.e., the ciphertext can be transformed only once.

Due to its transformation property, PRE schemes can be used in many applications,including simplification of key distribution [1], key escrow [2], distributed file systems [3], [4], multicast [5], anonymous communication [6], DFA-based FPRE system [7], and cloud computation [8], [9]. Recently, the research of cloud email system has become more and more popular in business and organizations as it allows an enterprise to rent the cloud SaaS service to build an email system with less costs and maintenance efforts. Indeed, it is much cheaper and scalable than traditional on-premises solution [10]–[13]. However, these solutions have a common drawback: the grant of content sharing capability, which is achieved through the generation of re-encryption key. Up to now, in all of the traditional identity based proxy re-encryption schemes, the generation of re-encryption key is generally divided into two ways: in uni-directional proxy re-encryption scheme, the key is generated by an authorized person A; in bi-directional scheme, it is generated by A and the recipient B [14]. Recently, Wang *et al*. [15] proposed a new scheme for the re-encryption key generation, where the key is generated by the sender S. This way has the advantage that the sender S can control the authorization granting process by using the random number, which is used in the encryption process to generate the proxy re-encryption key.

In this work, we propose a new identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy re-encryption, the sender S can control the people who can get the message and the sharing content of the messages.

A. Our Contribution

In this paper, based on Wang et al. 's proposal [15] and 3-linear map introduced in [17], we propose the IBPRE$^+$ scheme by using identity based encryption and 3-linear map, and analyse the proposal's property. Toward this construction, we first review the IBE scheme, and then we construct a new IBE scheme based on 3-linear Map. Based on that scheme, we propose our IBPRE$^+$ scheme. We roughly discuss the properties of our IBPRE$^+$ scheme. Finally, we demonstrate the potential application of our scheme to secure cloud data sharing.

B. Organization

We organize this paper as follows. In Section II, we first review the IBE scheme; secondly, we propose a new IBE scheme based on 3-linear map; then, we give our IBPRE$^+$ proposal and roughly discuss its properties. In Section III, we demonstrate the application of our scheme. In the last Section IV, we conclude our paper.

II. Our Proposed IBPRE+ Scheme

A. Review of the BB1 IBE Scheme

1) SetUp(1^k). Let G, G_T be a bilinear group of prime order p, and $e : G \times G \rightarrow G_T$ be the bilinear map. Given a security parameter 1^k as input, select a random generator g and $h, g_2 \in G$. Pick $\alpha \in Z_p^*$ and set $g_1 = g^\alpha$.
$$MK = \alpha, Pub = (g, g_1, g_2, h)$$
Let MK be a master secret key, and Pub be the public parameters.
2) KeyGen(MK, Pub, ID). Given master secret key $MK = \alpha$, public parameters Pub and an identity ID as input, the PKG picks $u \in Z_p^*$ and output an IBE secret key as
$$SK = (sk_1, sk_2) = (g_2^\alpha (g_1^{ID} h)^u, g^u)$$
3) Encrypt(ID, Pub, M). Given an identity ID, public parameter Pub and plaintext $M \in G_T$ as input, select $w \in Z_p^*$ and output an IBE ciphertext C.
$$C = (C_1, C_2, C_3) = (g^\omega, (g_1^{ID} h)^\omega, Me(g_1, g_2)^\omega)$$
4) Decrypt(SK, Pub, C). Given an IBE secret key SK, public parameters Pub and an IBE ciphertext C_I as input, output a plaintext M.
$$M = \frac{C_3 e(sk_2, C_2)}{e(sk_1, C_1)}$$

B. New IBE Scheme Based on 3-linear Map

1) SetUp(1^k). Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathcal{G}_1$. In addition, let $e_{a,b} : \mathcal{G}_a \times \mathcal{G}_b \rightarrow \mathcal{G}_{a+b} (a+b \leq 3)$ denote the 3-linear map. Given a security parameter 1^k as input, select a random generator g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^\alpha$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.
$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$
Let MK be a master secret key, and Pub be the public parameters.
2) KeyGen(MK, Pub, ID). Given master secret key $MK = \alpha$, public parameters Pub and an identity ID as input, the PKG picks $u \in Z_p^*$ and output an IBE secret key as
$$SK = (sk_1, sk_2) = (g_{12}^\alpha (g_{13}^{ID} h_{11})^u, g_{11}^u)$$
3) Encrypt(ID, Pub, M). Given an identity ID, public parameter Pub and plaintext $M \in G_T$ as input, select $w \in Z_p^*$ and output an IBE ciphertext C.
$$\begin{aligned} C &= (C_1, C_2, C_3, C_4) \\ &= (g_{11}^\omega, (g_{13}^{ID} h_{11})^\omega, M g_{31}^{\omega t}, g_{11}^t) \end{aligned}$$
4) Decrypt(SK, Pub, C). Given an IBE secret key SK, public parameters Pub and an IBE ciphertext C_I as input, output a plaintext M.
$$\begin{aligned} M &= \frac{C_3}{A}, A = e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4) \\ &= e_{21}(e_{11}(g_{12}, g_{13})^\omega, g_{11}^t) = e_{21}(g_{21}^\omega, g_{11}^t) \\ &= g_{31}^{\omega t} \end{aligned}$$

C. New IBE Scheme Based on 3-linear Map with Fixed Randomness

1) SetUp(1^k). Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathcal{G}_1$. In addition, let $e_{a,b} : \mathcal{G}_a \times \mathcal{G}_b \rightarrow \mathcal{G}_{a+b} (a+b \leq 3)$ denote the 3-linear map. Given a security parameter 1^k as input, select a random generator g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^\alpha$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.
$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$
Let MK be a master secret key, and Pub be the public parameters.
2) KeyGen(MK, Pub, ID). Given master secret key $MK = \alpha$, public parameters Pub and an identity ID as input, the PKG picks $u \in Z_p^*$ and output an IBE secret key as
$$SK = (sk_1, sk_2) = (g_{12}^\alpha (g_{13}^{ID} h_{11})^u, g_{11}^u)$$
3) Encrypt(ID, Pub, M). Given an identity ID, public parameter Pub and plaintext $M \in G_T$ as input, select a fixed random number $r \in Z_p^*$ and a random number $w \in Z_p^*$ and output an IBE ciphertext C.
$$\begin{aligned} C &= (C_1, C_2, C_3, C_4) \\ &= (g_{11}^{r\omega}, (g_{13}^{ID} h_{11})^{r\omega}, M g_{31}^{r\omega t}, g_{11}^t) \end{aligned}$$

4) Decrypt(SK, Pub, C). Given an IBE secret key SK, public parameters Pub and an IBE ciphertext C as input, output a plaintext M.

$$M = \frac{C_3}{A}, A = e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4)$$
$$= e_{21}(e_{11}(g_{12}, g_{13})^{r\omega}, g_{11}^{t})$$
$$= e_{21}(g_{21}^{r\omega}, g_{11}^{t}) = g_{31}^{r\omega t}$$

D. IBPRE$^+$ Scheme Based on 3-linear Map with Fixed Randomness

1) SetUp(1^k). Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathcal{G}_1$. In addition, let $e_{a,b} : \mathcal{G}_a \times \mathcal{G}_b \rightarrow \mathcal{G}_{a+b}(a+b \leq 3)$ denote the 3-linear map. Given a security parameter 1^k as input, select a random generator g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^{\alpha}$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.

$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$

Let MK be a master secret key, and Pub be the public parameters.

2) KeyGen(MK, Pub, ID_1). Given master secret key $MK = \alpha$, public parameters Pub and an identity ID_1 as input, the PKG picks $u \in Z_p^*$ and output an IBE secret key as

$$SK_{ID_1} = (sk_1, sk_2) = (g_{12}^{\alpha}(g_{13}^{ID_1}h_{11})^{u}, g_{11}^{u})$$

3) Encrypt(ID_1, Pub, M). Given an identity ID_1, public parameter Pub and plaintext $M \in G_T$ as input, select a fixed random number $r \in Z_p^*$ and a random number $w \in Z_p^*$ and output an IBE ciphertext C.

$$C = (C_1, C_2, C_3, C_4, C_5)$$
$$= (g_{11}^{r\omega}, (g_{13}^{ID_1}h_{11})^{r\omega}, Mg_{31}^{r\omega t}, g_{11}^{t}, g_{12}^{\omega t})$$

We can see the encrypter can decrypt the ciphertext by using g_{11}^{r} and computing $e_{21}(e_{11}(C_5, g_{13}), g_{11}^{r}) = e_{21}(g_{21}^{\omega t}, g_{11}^{r}) = g_{31}^{r\omega t}$.

4) ReKeyGen($Pub, r_{ID_1}, ID_1, ID_2$). On input the delegator's identity ID_1, delegatee's identity ID_2, public parameter Pub, the encrypter's fixed randomness r for ID_1, the encrypter generates the re-encryption key as following:

$$rk_{ID_1 \rightarrow ID_2} = (rk_1, rk_2, rk_3)$$
$$= (g_{11}^{-r}H(X)^{y}, g_{13}^{y}, IBE_{ID_2}(X))$$

where $H : \{0,1\}^* \rightarrow G_1$.

5) Reencrypt(Pub, C, r, ID_1, ID_2). On input the delegator's second level ciphertext and the re-encryption key, the proxy does the following:

$$C' = (C_1', C_2', C_3', C_4')$$
$$= (C_3 e_{21}(e_{11}(C_5, rk_1), g_{13}), rk_2 = g_{13}^{y},$$
$$C_5 = g_{12}^{\omega t}, IBE_{ID_2}(X))$$
$$= (Me(H(X)^{y}, g_{12}^{\omega t}, g_{13}), g_{13}^{y}, g_{12}^{\omega t},$$
$$IBE_{ID_2}(X))$$

6) Decrypt2(SK_{ID_1}, Pub, C). Given an IBE secret key SK, public parameters Pub and an IBE ciphertext C as input, output a plaintext M.

$$M = \frac{C_3}{A}, A = e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4)$$
$$= e_{21}(e_{11}(g_{12}, g_{13})^{r\omega}, g_{11}^{t})$$
$$= e_{21}(g_{21}^{r\omega}, g_{11}^{t}) = g_{31}^{r\omega t}$$

7) Decrypt1(SK_{ID_2}, Pub, C'). ID_2 first decrypt $C_4' = IBE_{ID_2}(X)$ to get $H(X)$ and then compute

$$A = e(C_3', H(X), C_2')$$
$$= e(g_{13}^{y}, H(X), g_{12}^{\omega t}), M = C_1'/A$$

E. Property Analysis

Here we discuss our IBPRE$^+$ scheme's property. According to the properties defined in [4], our scheme has the following properties:

1) Uni-directional: In our scheme, all of the re-encryption key is generated by the data sender S, so delegation from A → B does not allow re-encryption from B → A.
2) Non-interactive: The re-encryption keys can be generated by Alice using Bob's public key; no trusted third party or interaction is required.
3) Non-transitive: The proxy cannot re-delegate decryption rights. Because the proxy cannot get any information about the sender's private key, so he cannot produce $rk_{a\rightarrow c}$ from $rk_{a\rightarrow b}$ and $rk_{b\rightarrow c}$.
4) Message level based delegation: in our scheme, the encrypter can easily control which message shall be delegated by the proxy. For example, for $rk_{ID_1\rightarrow ID_2} = (g_{11}^{-r}H(X)^{y}, g_{13}^{y}, IBE_{ID_2}(X))$, if the encrypter wants to share the message with the delegatee, then he encrypts the message with randomness r, otherwise he encrypts message with other randomness. In this way our scheme can achieve message level based delegation.
5) Weak non-transferability: The proxy and a set of colluding delegatees cannot re-delegate decryption rights for all the ciphertexts of the delegator.

For instance, from $rk_{a\to b}$, sk_b, pk_c, although they can produce $rk_{a\to c}$ for fixed randomness r, but they can not produce $rk_{a\to c}$ for other ciphertexts not using randomness r, which partially solve the non-transferability.

III. IBPRE$^+$ for Secure Cloud Data Sharing

Based on our proposal, we can design a scheme useful for secure content sharing applications in Cloud. Thus, IBPRE$^+$ for secure cloud data sharing framework consists of the following algorithms: system initialization, key generation, data storage, data authorization and data recovery.

1) System initialization. First, the PKG selects a security parameter. On input the security parameter, the PKG generates some corresponding public parameters, which are outsourced to the system management Cloud server for other data users to share.
2) Key generation. The PKG generates the data owner and data users' private key by using the system parameters, user's identity and master secret key. Then, PKG sends the private key to the users via a secure channel.
3) Data store. When data owner Alice wants to outsource her private social multimedia content such as pictures, to the cloud, she first encrypts the pictures with ciphers suitable for JPEG or video encryption, and then encrypts the cipher's key with our IBPRE$^+$ scheme; finally, she outsources all the ciphertexts to the cloud storage server. Of course, the integrity of the outsourced data will be ensured by other techniques like provable data position, etc.
4) Data sharing. When data owner Alice want to share her personal pictures with her close friend Bob, she first generates the re-encryption keys for Bob by using Bob's identity, public parameters and her secret key, then outsource them to the cloud. The cloud storage server retrieves Alice's outsourced encrypted file, and then implements the re-encryption algorithm to send the re-encrypted ciphertext to Bob.
5) Data recovery. After receiving the re-encrypted ciphertexts, data sharer Bob decrypts them by using his own private key, thus he will get the cipher key for the pictures. Then, he requires to the cloud also to send him the encrypted pictures, and by using the retrieved cipher key, he can decrypt them to get the pictures.

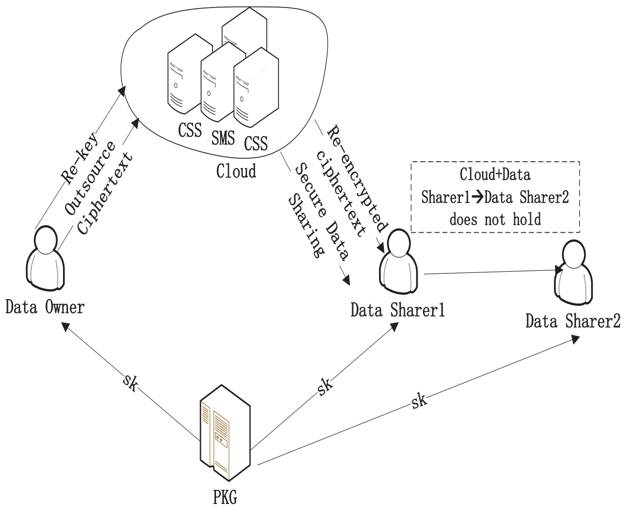

Fig. 1. Identity based proxy re-encryption plus for secure cloud data sharing

IV. Conclusion

In this paper, we propose a new primitive, called IBPRE$^+$, which is an identity based proxy re-encryption (PRE) scheme and propose the construction of such a concrete scheme. It can be seen as the dual of the traditional identity based proxy re-encryption. In the scheme, the data owner can control sharing capability in a flexible way by using random numbers used in the encryption process. Compared to traditional identity based proxy re-encryption schemes, our scheme has some advantages, and can be more appropriately adapted to some applications for content sharing, such as secure cloud data sharing. In our future research work, we would like to explore other aspects, such as giving formal security proof for our proposal, proposing more efficient schemes and implement the schemes in real Cloud environments, etc.

V. Acknowledgements

This work is supported by Natural Science Foundation of Shaanxi Province (Grant No. 2014JM8300).

References

[1] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 127–144, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany.

[2] Anca Ivan and Yevgeniy Dodis. Proxy cryptography revisited. In *NDSS 2003*, San Diego, California, USA, February 5–7, 2003. The Internet Society.

[3] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *NDSS 2005*, San Diego, California, USA, February 3–4, 2005. The Internet Society.

[4] 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, vol. 9, no. 1, pages 1–30. 2006.

[5] Yun-Peng Chiu, Chin-Laung Lei, and Chun-Ying Huang. Secure multicast using proxy encryption. In Sihan Qing, Wenbo Mao, Javier López, and Guilin Wang, editors, *ICICS 05*, volume 3783 of *LNCS*, pages 280–290, Beijing, China, December 10–13, 2005. Springer, Berlin, Germany.

[6] J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy re-encryption. Security and Communication Networks, vol. 5, no. 5, pp. 439-449, 2012.

[7] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S.Wong, and G. Yang. A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, 2014.

[8] Kaitai Liang, Joseph K. Liu, Duncan S. Wong, and Willy Susilo. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing. In Miroslaw Kutylowski and Jaideep Vaidya, editors, *ESORICS 2014, Part I*, volume 8712 of *LNCS*, pages 257–272, Wroclaw, Poland, September 7–11, 2014. Springer, Berlin, Germany.

[9] Ying Wang, Jiali Du, Xiaochun Cheng, Zheli Liu, and Kai Lin. Degradation and encryption for outsourced png images in cloud storage. International Journal of Grid and Utility Computing, vol. 7, no. 1, pp. 22-28, 2016.

[10] Shuaishuai Zhu and Xiaoyuan Yang. Protecting data in cloud environment with attribute-based encryption. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 91-97, 2015.

[11] Shu Guo and Haixia Xu. A secure delegation scheme of large polynomial computation in multi-party cloud. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp.1-7, 2015.

[12] Cristina Dutu, Elena Apostol, Catalin Leordeanu, and Valentin Cristea. A solution for the management of multimedia sessions in hybrid clouds. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 77-87, 2014.

[13] Meriem Thabet, Mahmoud Boufaida, and Fabrice Kordon. An approach for developing an interoperability mechanism between cloud providers. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 88-99, 2014.

[14] Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto. Identity-based proxy cryptosystems with revocability and hierarchical confidentialities. In Miguel Soriano, Sihan Qing, and Javier López, editors, *ICICS 10*, volume 6476 of *LNCS*, pages 383–400, Barcelona, Spain, December 15–17, 2010. Springer, Berlin, Germany.

[15] Xu An Wang, Yunlong Ge, and Xiaoyuan Yang. PRE^+: Dual of proxy re-encryption and its application. Cryptology ePrint Archive, Report 2013/872, 2013. `http://eprint.iacr.org/2013/872`.

[16] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang. Aconditional proxy broadcast re-encryption scheme supporting timed-release. ISPEC 2013, LNCS 7863, Springer, Heidelberg, pp. 132-146, 2013.

[17] S. Park, K. Lee, and D. H. Lee. New constructions of revocable identity based encryption from multilinear maps. IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1564-1577, 2015.