Fine-Grained Collaborative Access Control for IPFS with Efficient Revocation

Yifei Li(✉), Yinghui Zhang, and Qixuan Xing

School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Abstract. Access control is important for IPFS and collusion resistance is a basic requirement in traditional attribute-based encryption (ABE). However, in many emergency situations, conditional collaboration between multiple users is needed to decrypt ciphertext data. In addition, in order to make access control mechanisms suitable for the change of user attributes, it is necessary to construct ABE schemes that support attribute revocation. In this paper, a fine-grained collaborative decryption scheme that supports attribute revocation in IPFS storage (GORE-ABE) is proposed. In this scheme, the tree access policy is adopted, and the users are divided into different groups. The premise for successful decryption is that the users participating in the collaboration are in the same group and that the user attribute set satisfies the tree policy. The analysis results show that the GORE-ABE scheme is secure and efficient.

Keywords: Attribute-based encryption · IPFS · Collaborative decryption · Attribute revocation · Ciphertext update

1 Introduction

As time goes on, more people store massive data on cloud storage [1]. However, centralized cloud storage servers are prone to failure. Such as, the service provider interrupts service or removes the user's files on the grounds of violating the regulations [2]. In addition, cloud storage fees are getting higher and higher. Inter-Planetary File System (IPFS) has the characteristics of decentralization, semi-trust and automatic deletion of duplicate data [3]. Therefore, before uploading data to IPFS, users must use encryption algorithm to process their own private data [4–9]. Attribute-based encryption (ABE) is a traditional and widely used technology [10–13]. Although traditional ABE can realize collusion resistance, it requires conditional collaborative decryption by multiple users in many emergency situations. In view of this, Li et al. [14] proposed the concept of collaborative decryption of multiple users within a group. Specifically, users are grouped and only users in the same group can cooperate to decrypt, however, this scheme only implements coarse-grained access control policy [14]. Xue et al. [15] proposed group-oriented fine-grained collaborative operation scheme, but this scheme lacks necessary mechanisms such as attribute revocation and hence is not practical.

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 493–500, 2021.
https://doi.org/10.1007/978-3-030-89814-4_35

In summary, a scheme that only supports coarse-grained collaborative access control means that the scheme allows collaborative decryption of all user attributes within the same group. In a scheme that does not support fine-grained revocation, when a user logs out of the system but still has the decryption capability, this is undoubtedly a huge security hole [16, 17]. Therefore, it is vital to construct a fine-grained collaborative decryption scheme that supports efficient revocation (GORE-ABE).

Our Contribution. In this paper, a fine-grained collaborative decryption scheme that supports attribute revocation in IPFS storage (GORE-ABE) is proposed. Specifically, the GORE-ABE scheme uses ABE to realize fine-grained collaborative decryption of multiple users within a group. This scheme transfers the storage of mass data to IPFS server and avoids the occurrence of single point of failure. The scheme also implements efficient attribute revocation and ciphertext update. Next, the security and performance of the GORE-ABE are analyzed.

2 Preliminaries

2.1 Bilinear Maps

Two multiplicative cyclic groups G and G_T (g is the generator) are defined. A map $e : G \times G \rightarrow G_T$. The e is considered bilinear if it satisfies the following three requirements. Specific conditions are as follows: 1) Bilinearity; 2) Non-degeneracy; 3) Computability.

2.2 Application Scenario of GORE-ABE

The GORE-ABE scheme not only encrypts the privacy of users, but also realizes the decryption mechanism of single user and multi-user cooperation in emergency, which can be applied to the following scenarios. 1) Single decryption scenario: As in the traditional ABE scheme, a single user with sufficient access rights can decrypt. 2) Collaboration scenario: when a single user cannot decrypt, it can cooperate with other users with different attributes in the same group to decrypt. The process of collaborative decryption is as follows. First, the requester U_p tries to decrypt, and if the decryption fails, it will send a request to the group for cooperative decryption (broadcasting its own translation key $\mathbb{T}_p$). Translation key $\mathbb{T}_p$ are composed of group generators g, group identifiers θ_τ and random numbers (σ_p and $\mathbb{C}$) and can be used to assist in collaborative access scenarios. Second, a user U_p' in the same group (the collaborator U_p') responds to the request and calculates an intermediate ciphertext $e(g, g)^{\sigma_p' q_z(0)}$ with his private key $SK_p^{'}$. Thirdly, U_p' uses the received translation key U_p and its own translation key $\mathbb{T}_p^{'}$ and intermediate ciphertext $e(g, g)^{\sigma_p' q_z(0)}$ to compute the intermediate ciphertext $e(g, g)^{q_z(0) \cdot \sigma_p}$ and pass it back to the requester U_p. Finally, the requestor U_p receives the intermediate ciphertext $e(g, g)^{q_z(0) \cdot \sigma_p}$ and tries to decrypt it again. If it fails to decrypt, the requestor continues to request other users in the same group to join the collaboration until it can decrypt it. If it can decrypt it, the subsequent decryption operations will continue.

3 Construction of GORE-ABE

Since traditional ABE schemes [e.g. 9, 11, 12] do not support collaborative access control, and Xue et al. [15], which supports collaborative access control, cannot achieve fine-grained revocation at the user attribute level. Therefore, GORE-ABE scheme is proposed, and its system model is shown in Fig. 1, including four entities: IPFS storage server, Data Owners, Data Users and Authority Center (CA). The specific scheme is as follows.

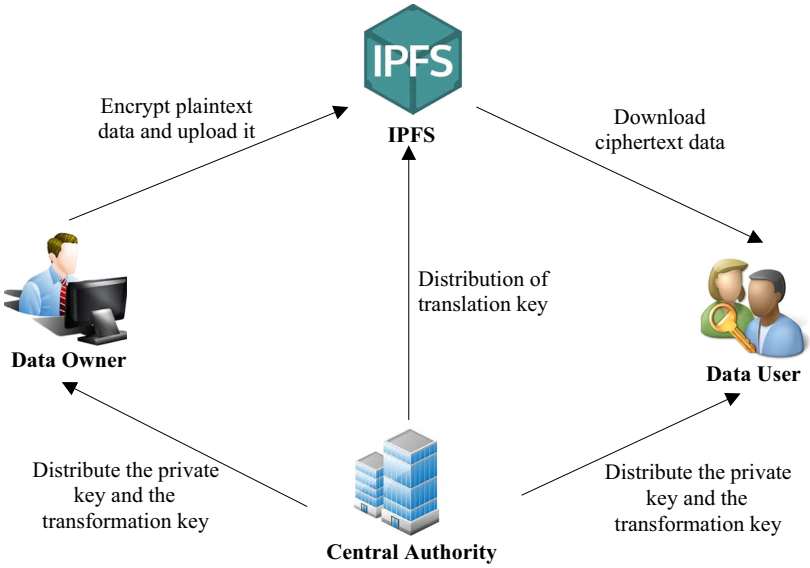

Fig. 1. System model

3.1 Setup

First, for each user group τ, CA defines the group secret key with random numbers $(\mathbb{A}, \mathbb{B}, \mathbb{C} \in \mathbb{Z}_{\mathbb{P}})$ and then defines map $e : G \times G \rightarrow G_T$. $\mathbb{H}$ is a hash function. Next, multiplicative cyclic groups G and G_T (g is generator) are picked by CA. Finally, In the scheme given ω project, selecting the secret key for each group $\theta_\tau \in \mathbb{Z}_{\mathbb{P}}$ and releasing unique identifier to each user U_p.

$$\text{Public key } PK = \left\langle \mathcal{D} = g^{\mathbb{B}}, \mathcal{F} = g^{\mathbb{C}}, J = g^{\frac{1}{\mathbb{B}}}, \mathcal{K} = g^{\frac{1}{\mathbb{C}}}, e(g,g)^{\mathbb{A}}, g, \mathbb{H}, G_T, G \right\rangle,$$
$$\text{Master key } MK = \left\langle g^{\mathbb{A}}, g^{\theta_1}, \ldots, g^{\theta_\tau}, \mathbb{B}, \mathbb{C} \right\rangle$$

3.2 KeyGen

The attribute set of user U_p is $S_p = \left\{a_{p,1}, \ldots, a_{p,\omega_p}\right\}$ ($a_{p,q}$ for S_p in the collection of the first q attributes, ω_p for S_p attributes in the number). First, CA use group key θ_τ marking

to the user. Then, the CA to users randomly selected $\sigma_p \in \mathbb{Z}_{\mathbb{P}}$, CA randomly select users attributes for $\sigma_{a_{p,q}} \in \mathbb{Z}_{\mathbb{P}}$ and attribute index $Q_{a_{p,q}} \in \mathbb{Z}_{\mathbb{P}}$, $1 \le q \le \omega_p$. Finally, the KeyGen outputs the translation key $\mathbb{T}_p$ [15] used for collaborative decryption and private key SK_p.

$$SK_p = \left\langle M_p = g^{\frac{\mathbb{A}+\theta_\tau}{\mathbb{B}}}, M_{p,q} = g^{\sigma_p}\mathbb{H}\left(a_{p,q}\right)^{\sigma_{p,q}}, M'_{p,q} = g^{\frac{\sigma_{p,q}}{Qa_{p,q}}}, 1 \le q \le \omega_p \right\rangle$$

$$\mathbb{T}_p = g^{\frac{\theta_\tau+\sigma_p}{\mathbb{C}}}$$

3.3 Encryption

For GORE-ABE scheme, mixed cryptography is used. The translation nodes [18] is set on the tree access policy, and only on the transformation node can multi-user collaboration decryption be allowed. $\mathbb{S}$ is the secret value in the tree $\mathcal{T}$.

Let $\mathbb{Y}$ and $\mathbb{X}$ be leaf node sets and non-leaf node sets in $\mathcal{T}$ respectively, and then get the ciphertext CT_μ.

$$CT_\mu = \left\langle \begin{array}{l} C = \mathcal{D}^{\mathbb{S}}, \overline{C} = \mathcal{F}^{\mathbb{S}}, \mathcal{T}, \forall x \in \mathbb{X} : \hat{C}_x = \mathcal{F}^{q_x(0)}, \\ \forall y \in \mathbb{Y} : C_y = g^{q_y(0)}, C'_y = \mathbb{H}(att(y))^{q_y(0)\cdot Qa_{p,q}}, \\ C' = \mu \cdot e(g,g)^{\mathbb{A}\mathbb{S}} \end{array} \right\rangle$$

3.4 Decryption

The requester U_p runs the decryption algorithm. If it can be decrypted, it is the traditional ABE decryption case alone. If it cannot be decrypted, it sends out the collaboration request signal to other users (collaborators) in the group to realize the multi-user cooperation decryption in an emergency U_p invokes the recursive decryption algorithm *DecNode*, inputs the user attribute set γ for decryption operation, and stores all the calculated node secret values in B_x.

- If x is a leaf node (attribute is p):

$$P_x = DecNode\left(CT_\mu, \gamma, u_p, x\right) = \frac{e\left(M_{p,q}, C_x\right)}{e\left(M'_{p,q}, C'_x\right)} = \frac{e\left(g^{\sigma_p}\mathbb{H}\left(a_{p,q}\right)^{\sigma_{p,q}}, g^{q_x(0)}\right)}{e\left(g^{\sigma_p}, \mathbb{H}\left(a_{p,q}\right)^{q_x(0)}\right)}$$

$$= e(g,g)^{\sigma_p q_x(0)}, att(x) = a_{p,q} \in S_p; \text{otherwise}, P_x = \perp.$$

- If x is a no-leaf node:

a) When z not translation nodes (not collaborate decryption), U_p try to decrypt separately (z is child node of x and attribute is p):

$$P_z = DecNode\left(CT_\mu, \gamma, u_p, z\right) = \frac{e\left(M_{p,q}, C_z\right)}{e\left(M'_{p,q}, C'_z\right)} = e(g,g)^{\sigma_p q_z(0)},$$

$$att(z) = a_{p,q} \in S_p; \text{otherwise}, P_z = \perp.$$

b) When z is translation nodes, GORE-ABE scheme can achieve multi-user collaboration decryption: The collaborator decrypts the secret value:

$$P'_z = DecNode\big(CT_\mu, \gamma, u_p, z\big) = \frac{e\big(M_{p,q}, C_z\big)}{e\Big(M'_{p,q}, C'_z\Big)} = e(g,g)^{\sigma'_p q_z(0)},$$

Then user U'_ps translation key $\mathbb{T}_p$ and own (collaborator's) translation key $\mathbb{T}'_p$ to convert P'_z into P_z containing U'_ps identity and sends it to U_p. P_z are as follow.

$$P_z = P'_z \cdot e(\hat{C}_z, \frac{\mathbb{T}_p}{\mathbb{T}'_p}) = e(g,g)^{\sigma'_p q_z(0)} \cdot e(g^{\mathbb{C}} g^{q_z(0)}, g^{\frac{\theta_\tau + \sigma_p}{c}} \Big/ g^{\frac{\theta_\tau + \sigma'_p}{c}})$$
$$= e(g,g)^{q_z(0)\cdot\sigma_p}$$

- U_p merge user attribute private key set and continue decryption operation using Lagrange interpolation formula:

$$P_x = \prod_{z\in B_x} P_z^{\Delta_{index(z),\{index(z)\}(0)}} = e(g,g)^{\sigma_p q_z(0)}, \text{among them:}$$
$$\Delta_{p,S(x)} = \prod_{q\in S, q\neq p} \frac{x-q}{p-q}$$

Then, U_p runs the recursive algorithm to decrypt the root node r as follows:

$$P_r = DecNode\big(CT_\mu, \gamma, r, u_i\big) = e(g,g)^{\sigma_p \cdot \mathbb{S}}.$$

Continue decrypting, output:

$$P = \frac{e\big(\overline{C}, \mathbb{T}_p\big)}{P_r} = \frac{e\Big(g^{\mathbb{C}\cdot q_r(0)}, g^{\frac{\theta_\tau}{\mathbb{C}}} \cdot g^{\frac{\sigma_p}{\mathbb{C}}}\Big)}{e(g,g)^{\sigma_p \cdot q_r(0)}} = e(g,g)^{\theta_\tau \cdot \mathbb{S}},$$

U_p download the ciphertext from IPFS and decrypt the symmetric key μ:

$$\mu = \frac{P\cdot C'}{e\big(C, M_p\big)} = \frac{e(g,g)^{\theta_\tau\cdot\mathbb{S}} \cdot \mu \cdot e(g,g)^{\mathbb{S}\mathbb{A}}}{e\Big(g^{\mathbb{B}\mathbb{S}}, g^{\frac{\mathbb{A}+\theta_\tau}{\mathbb{B}}}\Big)}.$$

- Finally, U_p uses μ to decrypt $Enc_\mu(M)$ to recover the plaintext M.

3.5 KeyUpdate

If an attribute ε is revoked, the corresponding index $Qa_{p,q}$ and ciphertext CT_μ are refactored. CA randomly chosen $Q'_{a_{p,q}} \in \mathbb{Z}_\mathbb{P}$ (It's different from $Qa_{p,q}$) and sent it to contain attributes ε for all users. After receiving it, the relevant users update their private keys: $M'_{p,q} = g^{\frac{Qa_{p,q}}{Q'a_{p,q}}}$. However, users without ε are not affected and $\mathbb{T}_p = g^{\frac{\theta_\tau+\sigma_p}{\mathbb{C}}}$ does not need to be updated.

CA sends the new attribute index $Q'_{a_{p,q}} \in \mathbb{Z}_\mathbb{P}$ to IPFS, which updates the ciphertext by introducing random number $\varphi(\varphi \in \mathbb{Z}_\mathbb{P})$. The updated ciphertext:

$$CT'_\mu = \left\langle \begin{array}{l} \forall x \in \mathbb{X} : \hat{C}_x = \mathcal{F}^{q_x(0)+\varphi}, C = \mathcal{D}^{(\mathbb{S}+\varphi)}, \overline{C} = \mathcal{F}^{\mathbb{S}+\varphi}, \mathcal{T}, \\ \forall y \in \mathbb{Y} : C_y = g^{q_y(0)+\varphi}, C'_y = \mathbb{H}(att(y))^{(q_y(0)+\varphi)\cdot Qa_{p,q}}, \\ C' = \mu \cdot e(g,g)^{\mathbb{A}(\mathbb{S}+\varphi)} \end{array} \right\rangle$$

4 Security Analysis

The failure-prone nature of cryptography has led to a widespread belief that these systems should be designed and analyzed in a formal way. Next, we consider the following security features.

Data Confidentiality: IND games are often used to describe the semantic security of cryptographic schemes. In such a game, the algorithm is said to be provably security if the two messages in the safe game are indistinguishable to the opponent [19]. GORE-ABE scheme roughly is the same as the data confidentiality proof in reference [12, 15], so the security of GORE-ABE scheme is the same as that of reference [12, 15], that is, it realizes the provable security under the general group model.

Anti-User Collusion: GORE-ABE scheme uses parameters such as group identifier, user random number and user attribute random number to resist user collusion.

Controlled Collaboration Within a Group: Only users in the same group can cooperate to decrypt, and all other actions are considered as collusion attacks.

Private Key Confidentiality: Translation key $\mathbb{T}_p$ [18] are composed of group generators g, group identifiers θ_τ and random numbers (θ_τ and $\mathbb{C}$) and can be used to assist in collaborative access scenarios without users revealing their private keys SK_p.

Secure Revocation of User Attribute: GORE-ABE scheme can effectively resist user collusion.

5 Performance Evaluation

The performance of GORE-ABE scheme is analyzed by comparing it with the scheme proposed by Xue et al. [15]. In short, the GORE-ABE scheme maintains high efficiency on the basis of realizing attribute revocation.

5.1 Computational Complexity

The computation overhead of addition and multiplication operation is very small, so the main operations in the algorithm include exponentiations and pairings. Although a small amount of exponentiations is added in GORE-ABE scheme, the computational overhead is not increased and the algorithm is more practical. In addition, the ciphertext update algorithm is executed by IPFS.

For convenience, expressed in P_a bilinear mapping, expressed in E_x index operation, the number of user attributes in W_n said with W_c said the number of attributes associated with the access structure expressed in W_y number of user attributes for decryption in W_l from the root node to leaf node between the number of leaf nodes, expressed in T_r convert the number of nodes, with $T_r^{'}$ for decryption of the conversion of the node number. In Table 1, we give the theoretical computation overhead above two schemes.

Table 1. Computation overhead.

Phase	Xue et al. scheme	Ours
Setup	$(5+\omega)E_x + P_a$	$(5+\omega)E_x + P_a$
KeyGen	$(2W_n + 3)E_x$	$(2W_n + 3)E_x$
Encryption	$(2W_c + 3 + T_r)E_x$	$(3W_c + 3 + T_r)E_x$
Decryption	$(2W_y + 2 + T_r^{'})P_a + (W_l + W_y)E_x$	$(2W_y + 2 + T_r^{'})P_a + (W_l + W_y)E_x$
KeyUpdate	N/A	E_x

5.2 Computational Complexity

The storage costs, communication costs, encryption and decryption time, ciphertext size and other parameters of GORE-ABE scheme are consistent with those of Xue et al. [15].

6 Conclusion

In this paper, we propose a fine-grained collaborative operation scheme that allows multiple users within a group (GORE-ABE). This scheme transfers the storage of mass data to IPFS and avoids single point of failure. In addition, the scheme also implements the user's attribute revocation and ciphertext update, which further enhances the practicability of the scheme. The GORE-ABE scheme is secure and has a broad prospect in practical application.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (62072369, 62072371, 61772418), the Innovation Capability Support Program of Shaanxi (2020KJXX-052), the Shaanxi Special Support Program Youth Top-notch Talent Program, the Key Research and Development Program of Shaanxi (2019KW-053, 2020ZDLGY08-04, 2021ZDLGY06-02), and Sichuan Science and Technology Program under Grant 2017GZDZX0002.

References

1. Liang, Y., Cheng, H., Chen, W.: Building energy consumption data index method in cloud computing environment. Int. J. Perform. Eng. **16**(5), 747–756 (2020)
2. Wu, J., Ping, L., Ge, X., et al.: Cloud storage as the infrastructure of cloud computing. In: 2010 International Conference on Intelligent Computing and Cognitive Informatics, pp. 380–383. IEEE (2010)
3. Benet, J.: Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561 (2014)
4. Xiong, J., Bi, R., Zhao, M., et al.: Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles. IEEE Wirel. Commun. **27**(3), 24–30 (2020). https://doi.org/10.1109/MWC.001.1900463

5. Tian, Y., Wang, Z., Xiong, J., et al.: A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Trans. Industr. Inf. **16**(9), 6193–6202 (2020). https://doi.org/10.1109/TII.2020.2965975
6. Xiong, J., Ma, R., Chen, L., et al.: A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Trans. Industr. Inf. **16**(6), 4231–4241 (2020)
7. Tian, Y., Li, Q., Hu, J., Lin, H.: Secure limitation analysis of public-key cryptography for smart card settings. World Wide Web **23**(2), 1423–1440 (2019). https://doi.org/10.1007/s11280-019-00715-8
8. Chen, Z., Tian, Y., Peng, C.: An incentive-compatible rational secret sharing scheme using blockchain and smart contract. Sci. China Inf. Sci. **64**(10), 1–21 (2021). https://doi.org/10.1007/s11432-019-2858-8
9. Xiong, J., Chen, X., Yang, Q., et al.: A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. IEEE Trans. Netw. Sci. Eng. **7**(4), 2347–2360 (2020)
10. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (eds.) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494. Springer, Heidelberg. https://doi.org/10.1007/11426639_27
11. Zhang, Y., Chen, X., Li, J., et al.: Attribute-based data sharing with flexible and direct revocation in cloud computing. KSII Trans. Internet Inf. Syst. **8**(11), 4028–4049 (2014)
12. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP 2007), pp. 321–334. IEEE (2007)
13. Zhang, Y., Zheng, D., Chen, X., et al.: Efficient attribute-based data sharing in mobile clouds. Pervasive Mob. Comput. **28**, 135–149 (2016)
14. Li, M., Huang, X., Liu, J.K., Xu, L.: GO-ABE: group-oriented attribute-based encryption. In: Au, M.H., Carminati, B., Kuo, C.C.J. (eds.) Network and System Security. NSS 2015. Lecture Notes in Computer Science, vol. 8792. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11698-3_20
15. Xue, Y., Xue, K., Gai, N., et al.: An attribute-based controlled collaborative access control scheme for public cloud storage. IEEE Trans. Inf. Forensics Secur. **14**(11), 2927–2942 (2019)
16. Zhang, Y., Deng, R.H., Xu, S., et al.: Attribute-based encryption for cloud computing access control: a survey. ACM Comput. Surv. (CSUR) **53**(4), 1–41 (2020)
17. Hur, J., Noh, D.K.: Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans. Parallel Distrib. Syst. **22**(7), 1214–1221 (2010)
18. Bobba, R., Khurana, H., Prabhakaran, M.: Attribute-sets: a practically motivated enhancement to attribute-based encryption. In: Backes, M., Ning, P. (eds.) Computer Security – ESORICS 2009. ESORICS 2009. Lecture Notes in Computer Science, vol. 5789. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04444-1_36
19. Pointcheval, D.: Provable security for public key schemes. In: Contemporary Cryptology. Advanced Courses in Mathematics - CRM Barcelona (Centre de Recerca Matemàtica). Birkhäuser Basel (2005). https://doi.org/10.1007/3-7643-7394-6_4