View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Institutional Knowledge at Singapore Management University

Singapore Management University
Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems | School of Information Systems

8-2018

A fine-grained attribute based data retrieval with proxy re-encryption scheme for data outsourcing systems

Hanshu HONG
Nanjing University of Posts and Telecommunications

Ximeng LIU
Singapore Management University, xmliu@smu.edu.sg

Zhixin SUN
Nanjing University of Posts and Telecommunications

DOI: https://doi.org/10.1007/s11036-018-1102-3

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research


Part of the Databases and Information Systems Commons, and the Information Security Commons

Citation

HONG, Hanshu; LIU, Ximeng; and SUN, Zhixin. A fine-grained attribute based data retrieval with proxy re-encryption scheme for data outsourcing systems. (2018). *Mobile Networks and Applications*. 1-6. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/4124

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Mobile Networks and Applications
https://doi.org/10.1007/s11036-018-1102-3

A Fine-Grained Attribute Based Data Retrieval with Proxy Re-Encryption Scheme for Data Outsourcing Systems

Hanshu Hong[1] · Ximeng Liu[2] · Zhixin Sun[1]

Abstract
Attribute based encryption is suitable for data protection in data outsourcing systems such as cloud computing. However, the leveraging of encryption technique may retrain some routine operations over the encrypted data, particularly in the field of data retrieval. This paper presents an attribute based date retrieval with proxy re-encryption (ABDR-PRE) to provide both fine-grained access control and retrieval over the ciphertexts. The proposed scheme achieves fine-grained data access management by adopting KP-ABE mechanism, a delegator can generate the re-encryption key and search indexes for the ciphertexts to be shared over the target delegatee's attributes. Throughout the process of data sharing, the data are transferred as ciphers thus the server and unauthorized users cannot acquire the sensitive information of the encrypted data so the privacy and confidentiality can be protected. By security analysis, the proposed scheme meets the security requirements confidentiality, keyword semantic security as well as collusion attack resistance.

Keywords Attribute based data retrieval · Proxy re-encryption · Collusion resistance · Secure

1 Introduction

The developments of several new computing techniques such as distributed computing [1] have made data sharing more and more convenient among users. However, while users are enjoying the convenience brought by these techniques, they are also faced with a series of issues related to information security. These issues arise from the fact that most computing resources providers are operated by commercial institutes which are very likely to be outside of the trusted domain of data owners. Although traditional "one-to-one" data encryption techniques can preserve the confidentiality and integrity of the sensitive data [2], they are not able satisfy a series of new demands emerging in these scenarios, such as high efficient data encryption, fine-grained access control, etc. To be a new type of public key cryptosystem, attribute based cryptosystem provides a good method to tackle the above problems. In attribute based cryptosystem, a data owner does not have to know the exact identity of each receiver, he can realize fine-grained data access control by describing the ciphertexts or target users using attributes. Consequently, attribute based cryptosystem is especially suitable for data protection in distribute network scenarios.

So far, researches domestic and abroad have proposed many schemes on attribute based cryptosystems, including attribute based encryption schemes, attribute based signature schemes, attribute based signcryption schemes and attribute based proxy schemes, etc. These schemes are equipped with rich functionalities and favorable security properties.

However, traditional encryption techniques may retrain some routine operations over the encrypted data, particularly in the field of data retrieval [3, 4]. Since data are stored as ciphers in the data outsourcing center and the quantity is very large [5–9], it is inconvenient for a data receiver to seek out the target files and contents hidden in the ciphers. One method is that a data receiver decrypts all the possible ciphertexts and search the desired file over the plaintexts, but the decrypt operation over the possible ciphers will add considerable computation. Thus, a scheme which provides both the function of proxy re-encryption and data retrieval is urgently to be proposed.

In this paper, we present an attribute based date retrieval with proxy re-encryption (ABDR-PRE) to provide both fine-grained access control and retrieval over the ciphertexts. Our

✉ Hanshu Hong
2014070244@njupt.edu.cn

[1] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

[2] Singapore Management University, Singapore 178902, Singapore

scheme achieves fine-grained data access management by adopting KP-ABE mechanism, a delegator can generate the re-encryption key and search indexes for the ciphertexts to be shared over the target delegatee's attributes. Our scheme also introduces key updating mechanism by cutting the system lifespan into several time periods and the re-encryption keys are time-bounded. A re-encryption key from a previous time slice cannot generate a valid ciphertext for the current time period so that the authority of the server can be securely insulated. Throughout the process of data sharing, the data are transferred as ciphers thus the server and unauthorized users cannot acquire the sensitive information of the encrypted data so the privacy and confidentiality can be protected. By security analysis, our scheme meets the security requirements confidentiality, keyword semantic security as well as collusion attack resistance.

2 Related works

2.1 Attribute based encryption

In 2005, Sahai et al. proposed the first ABE scheme which adopted threshold as the access structure [10]. Later, Goyal and Bethencourt et al. designed new access structures named KP-ABE [11] and CP-ABE [12] respectively, which can provide more flexible managements over the encrypted data. Based on their constructions, researchers have proposed many valuable schemes. Waters et al. in [13] presented a new novel CP-ABE scheme which applied LSSS to satisfy the demands of access control management and proved their scheme to be secure under d-BDHE assumptions. Li et al. in [14] proposed a paralyzed CP-ABE and applied their scheme in cloud environments. Equipped with AES algorithm, the processes of key generation and encryption became more efficient. Reedy et al. in [15] designed a secure architecture for digital health system by taking the advantage of CP-ABE. Their scheme allowed a public auditor to conduct verification of the health data without leaking users' personal information. Furthermore, their scheme solved the issue of key escrow by introducing two key generations. Liu et al. in [16] proposed a functional CP-ABE which not only supported attribute revocation but also realized black box piracy tracing when key exposure occurred. Meanwhile, there is no need for system manager to define the global attribute set in advance, so the proposed scheme is equipped with high scalability and extensibility. Yang et al. in [17] pointed out that the considerable cost of decryption and revocation were two obstacles which could prevent the further application of CP-ABE. They also designed a CP-ABE scheme for cloud access which adopted several centers to manage users' attributes. The efficiency of attribute revocation and decryption had been improved in this mode. Padhya et al. in [18] extended the functions of CP-ABE by hiding the access policies. Besides, it was resisted to collusion attack conducted by malicious users. Miyaji et al. in [19] presented a novel dual-policy ABE by combing the merits of both CP-ABE and KP-ABE. Their scheme was equipped with constant length of ciphertext and testified to be secure under q-BDHE assumption. Cheng et al. in [20] designed a secure and revocable CP-ABE scheme. The core idea of their scheme was to separate the original files into several data segments before encryption. When attribute revocation occurred, data owner only needs to re-encrypt the ciphertexts which accorded with the attributes to be altered. This technique avoided the considerable computation burden of re-encrypting all the ciphertexts and was proved to be more efficient by conducting experiments on hardware. Qiu et al. in [21] realized the function of hidden policy which protected the confidentiality of both ciphertexts and access structures. By conducting simulation, the authors claimed the overall effectiveness of their scheme was raised. Hong et al. in [22] applied ABE to mobile multimedia networks and gained time-bounded security by leveraging a flexible key refreshing mechanism. Apart from the above research directions, researchers have also presented schemes with various functions such as ABE constructed on lattice, ABE without pairings [23], etc.

2.2 Proxy re-encryption

A proxy re-encryption protocol consists of three entities: delegator, proxy server and delegatee. Delegator has the privilege of decrypting the original ciphertext. What's more, delegator can generate a proxy key using his private key and the target delegatee's public key. With the proxy key and the original ciphertext, a semi-trusted server can generate a new ciphertext which is encrypted by the delegatee's public key. Throughout the re-encryption process the data are transferred as ciphers so the confidentiality and privacy during data communication can be guaranteed.

Until now, researchers have presented many re-encryption schemes with multiple functions [24]. These schemes can be divided into directional and unidirectional according to the re-encryption directions. From the prospective of cryptosystem, these schemes can be classified as identity based proxy re-encryption, attribute based proxy re-encryption, etc.

2.3 Searchable encryption

Searchable encryption is an efficient technique to provide keyword search function over the encrypted data. The framework of a searchable encryption usually involves three entities: data owner, user and server. Data owner generates the ciphertext along with the search indexes of the corresponding ciphertext, then sends them to be stored in the server. User generates the trapdoor for the required ciphertext using the private key he owns and delivers the trapdoor to the server. Server returns the

corresponding ciphertext to user if the trapdoor matches with the given search index. Due to its properties, searchable encryption is particularly suitable for information retrieval in data outsourcing systems such as cloud computing. From the prospective of cryptosystems, existing works referring to searchable encryption can be divided into symmetric cryptosystem searchable encryption, traditional public cryptosystem searchable encryption, identity based searchable encryption, etc.

3 Models and definitions

For the convenience of description, we denote some notations which are listed in Table 1.

3.1 Syntax

Our proposed ABDR-PRE consists of ten algorithms:

$Setup(1^{\varphi} \rightarrow MK, PK)$	It takes a security parameter as input and outputs PK, MK.
$Key\ generation(MK, \gamma_i \rightarrow SK)$	It takes MK and an user's γ_i as input, it outputs SK of the user.
Key update	This algorithm is an interaction between AA and user. It refreshes user's SK from previous time slice to the newest version.
$Encrypt(M, A_i, PK \rightarrow CT)$	It takes M and the target A_i as input and outputs CT.
$Re-Key\ generation(SK, A_j, PK \rightarrow rk)$	It takes the delegator's SK and the delegatee's A_j as input, it outputs rk.
$Search\ index\ generation(w, A_j, PK \rightarrow IN)$	It takes w related to a ciphertext and the delegatee's A_j as input and outputs IN.
$Re-Encrypt(CT, rk \rightarrow CT^{'})$	It takes rk and CT as input and outputs $CT^{'}$.
$Trapdoor(SK, w, PK \rightarrow TR)$	It takes delegatee's SK and w as input and outputs TR.
$Test(TR, IN, PK \rightarrow CT^{'})$	It takes TR, IN as input and returns $CT^{'}$ if TR is valid.
$Decrypt(CT^{'}, SK \rightarrow M)$	It takes $CT^{'}$ and the delegatee's SK as input and outputs M.

3.2 Security properties

Confidentiality: This security property can be proved by a game described as follows.

Setup: *Adversary* claims a challenging attribute set S_c. *Challenger* runs setup algorithm and sends public parameters to *Adversary*.

Table 1 Notations

Abbreviation	Meaning
φ	Security parameter
AA	Attribute authority
MK	System master key
PK	System public parameters
f	Hash functions
A_i	Single attribute "i"
t	Time slice
S	Attribute set
γ_i	Access structure containing A_i
sk	User's private key
rk	Re-encryption key
w	Keyword
IN	Search index
TR	Trapdoor
CT	Original ciphertext
$CT^{'}$	Proxy ciphertext
M	Plaintext

Key generation query: On input the access structure picked by *Adversary*, *Challenger* outputs the corresponding private key and sends it back to *Adversary*.

$Re-Key\ generation\ query$: On input an access structure and an target attribute set, *Challenger* returns rk to *dversary* .

$Re-Encrypt\ query$: *Adversary* delivers rk and CT to *Challenger* and obtains $CT^{'}$.

Challenge: *Adversary* generates M_0, M_1 of equal sizes. *Challenger* picks $\sigma \in \{0, 1\}$, encrypts M_σ over S_c and returns CT_σ to *Adversary*.

Adversary outputs $\sigma^{'}$ as the guess of σ and wins the game if $\sigma^{'} = \sigma$.

The advantage of *Adversary* can be defined by $Adv = \left|Pr\left[\sigma^{'} = \sigma\right] - \frac{1}{2}\right|$.

Keyword semantic security: This security property can be proved by a game described as follows.

Setup : *Challenger* runs *Setup* to obtain the public parameters in the game

Adversary claims γ_{ic} *to* be the challenging structure.

Trapdoor query: *Challenger* can obtain the trapdoor of several keywords for attribute set S by running *Trapdoor* algorithm and sends the results back to *Adversary*.

Challenge : *Adversary* picks keywords w_0, w_1 which are not from previous queries.

Challenger picks $\sigma \in \{0, 1\}$ and runs *Search index generation* algorithm to get the IN of w_σ.

Adversary outputs σ^* as a guess of σ. If $\sigma^* = \sigma$ then *Adversary* wins the game.

The advantage of *Adversary* can be defined by $Adv(A) = |Pr[\sigma^* = \sigma] - \frac{1}{2}|$.

Collusion resistance: This security property requires that it is computational infeasible for a sever and a malicious delegatee to collude in order to calculate the private key of a delegator.

4 Constructions

Setup: AA defines two p order groups G_1, G_2. Let $\hat{e}: G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing and g_1, g_2 are two generators of G_1. Defines a global attribute set. Defines hash functions: $f_1: \{0,1\}^* \rightarrow G_1$, $f_2: \{0,1\}^* \rightarrow Z_p^*$. Randomly chooses $h, y \in Z_p^*$ and computes $Y = \hat{e}(g_1, g_2)^y, H = {g_2}^h$. Picks a_i for each attribute in the system and let $A_i = {g_1}^{a_i}, A_i' = {g_2}^{a_i}, AH_i' = {g_2}^{ha_i}$.

$MK = \{y, l, a_i\}$ and $PK = \{p, G_1, G_2, g_1, g_2, \hat{e}, f_1, f_2, H, AH_i', Y, A_i, A_i'\}$.

Key generation:For a user holding γ_i, AA picks $r, r_i \in Z_p^*$ and defines a polynomial for each node in γ_i. The method of polynomial generation is similar to Water's scheme in [11]. Then the initial SK of a use can be defined by $SK = \left\{D_i = {g_1}^{\frac{q_x(0)}{a_i}} \cdot f_1(A_i, t_0)^h, i \in \gamma_i\right\}$.

Key update: AA computes $\left\{U_i = \left(\frac{f_1(A_i, t_{m+1})}{f_1(A_i, t_m)}\right)^h, i \in \gamma_i\right\}$ when system enters t_m from t_{m+1}. User updates SK by calculating $D_i \cdot U_i$.

Encrypt: For M with the target $\{A_i\}$, data owner selects $s \in Z_p^*$ then computes:

$$\begin{aligned} C_0 &= M \cdot Y^s, C_{1,i} = {A_i}'^s \\ C_{2,i} &= f_1(A_i, t_m)^s, C_3 = {g_1}^s \\ C_{4,i} &= {AH_i}'^s \end{aligned} \tag{1}$$

Then data owner sends the $CT = \{C_0, C_{1,i}, C_{2,i}\}$ to server.

Re − Key generation:When a delegator holding γ_i intends to share CT over $\{A_j\}$, then the delegator picks $k, x_1 \in Z_p^*, X \in G_2$ and generates rk as follows:

$$\begin{aligned} rk_{1,i} &= {D_i}^{f_2(X)} \cdot {g_1}^k \\ rk_{2,i} &= {A_i}'^k \\ rk_{3,i} &= f_1(A_i, t_m)^{f_2(X)} \\ C_1' &= \left\{{A_j}'^{x_1}, f_1(A_j, t_m)^{x_1}, X \cdot Y^{x_1}\right\} \\ rk &= \left\{rk_{1,i}, rk_{2,i}, rk_{3,i}, C_1'\right\} \end{aligned} \tag{2}$$

Search index generation:For w, the delegator picks $x_2 \in Z_p^*$ and generates IN of w as follows:

$$\begin{aligned} IN_0 &= Y^{x_2 f_2(w)}, IN_1 = {g_1}^{x_2} \\ IN_{2,j} &= {A_i}'^{x_2}, IN_{3,j} = f_1(A_j, t_m)^{x_2} \end{aligned} \tag{3}$$

The delegator sends $IN = \{IN_0, IN_1, IN_2, IN_{3,j}\}$ to server.

Re − Encrypt:Upon receiving rk from delegator, server calculates:

$$\begin{aligned} C_2' &= \prod_{i \in \gamma_i} \hat{e}(rk_{1,i}, C_{1,i}) \cdot \hat{e}(C_3, rk_{2,i})^{-1} CT' \\ &= \left\{C_0, C_1', C_2'\right\} \end{aligned} \tag{4}$$

Trapdoor: When a delegatee holding γ_j wants to make a search on the ciphertext containing w, the delegatee picks $l \in Z_p^*$ and generates TR as follows:

$$\begin{aligned} TR_{1,j} &= \left(D_j \cdot {g_1}^l\right)^{f_2(w)} \\ TR_{2,j} &= {A_i}'^{lf_2(w)} \\ TR_3 &= {HA_i}'^{f_2(w)} \end{aligned} \tag{5}$$

Then the delegatee sends $TR = \{TR_1, TR_{2,j}, TR_{3,j}, TR_4, j \in \gamma_j\}$ to the server.

Test:The server verifies whether (6) holds or not:

$$\prod_{j \in \gamma_j} \hat{e}(IN_{2,j}, TR_{1,j}) \cdot \hat{e}(IN_{3,j}, TR_{3,j})^{-1} \cdot \hat{e}(IN_1, TR_{2,j}) = IN_0 \tag{6}$$

If equation (6) holds then the trapdoor is valid and the server sends the CT' to the delegatee.

Decrypt: After receiving the CT', the delegatee calculates X by computing:

$$X \cdot Y^{x_1} \cdot \prod_{j \in \gamma_j} \hat{e}\left({A_j}'^{x_1}, D_j\right) \cdot \hat{e}\left({AH_j}', f_1(A_j, t_m)^{x_1}\right)^{-1} \tag{7}$$

Then recovers M by computing:

$$M = \frac{C_0}{{C_2}'^{(f_2(X))^{-1}}} \tag{8}$$

5 Discussion

5.1 Correctness proof

Firstly, CT is a valid original ciphertext and an authorized user can recover the plaintext by calculating:

$$M = C_0 \cdot \prod_{i \in \gamma_i} \hat{e}(D_i, C_{1,i})^{-1} \cdot \hat{e}\left(C_{2,i}, {AH_i}'\right)^{-1} \tag{9}$$

The calculation involves the invoking of recursion and Lagrange interpolation function which have already been fully examined in [11], so in this paper the detailed calculation process will not be repeated.

Then we will prove the correctness of proxy-encryption and data retrieval.

It can be figured out from (8) that $C_2^{'}$ and X are two essential elements for recovering M.

From our constructions, $C_2^{'} = Y^{f_2(X)s}$ and the proof is demonstrated in (10).

$$
\begin{aligned}
C_2^{'} &= \prod_{i\in\gamma_i} \hat{e}\left(rk_{1,i}, C_{1,i}\right)\cdot\hat{e}\left(C_3, rk_{2,i}\right)^{-1}\cdot\hat{e}\left(rk_{3,i}, C_{4,i}\right)^{-1} \qquad (10)\\
&= \prod_{i\in\gamma_i} \hat{e}\left(D_i^{f_2(X)}\cdot g_1^{k}, A_i^{'s}\right)\cdot\hat{e}\left(g_1^{s}, A_i^{'k}\right)^{-1}\cdot\hat{e}\left(f_1(A_i,t_m)^{f_2(X)}, g_2^{sha_i}\right)^{-1}\\
&= \prod_{i\in\gamma_i} \hat{e}\left(g_1^{\frac{q_x(0)f_2(X)}{a_i}}\cdot f_1(A_i,t_m)^{hf_2(X)}\cdot g_1^{k}, A_i^{'s}\right)\cdot\hat{e}\left(g_1^{s}, A_i^{'k}\right)^{-1}\cdot\hat{e}\\
&\left(f_1(A_i,t_m)^{f_2(X)}, g_2^{sha_i}\right)^{-1} = \prod_{i\in\gamma_i} \hat{e}\left(g_1^{\frac{q_x(0)f_2(X)}{a_i}}\cdot f_1(A_i,t_m)^{hf_2(X)}, A_i^{'s}\right)\cdot\hat{e}\\
&\left(f_1(A_i,t_m)^{f_2(X)}, g_2^{sha_i}\right)^{-1} = \prod_{i\in\gamma_i} \hat{e}\left(g_1^{\frac{q_x(0)f_2(X)}{a_i}}, g_2^{a_i s}\right)\\
&= \prod_{i\in\gamma_i} \hat{e}(g_1,g_2)^{q_x(0)f_2(X)s} = \hat{e}(g_1,g_2)^{yf_2(X)s} = Y^{f_2(X)s}
\end{aligned}
$$

The value of X can also be calculated via (7) and the proof is demonstrated in (11):

$$
\begin{aligned}
&X\cdot Y^{x_1}\cdot\prod_{j\in\gamma_j}\hat{e}\left(A_j^{'x_1}, D_j\right)\cdot\hat{e}\left(AH_j^{'}, f_1\left(A_j,t_m\right)^{x_1}\right)^{-1} \qquad (11)\\
&= X\cdot Y^{x_1}\cdot\prod_{j\in\gamma_j}\hat{e}\left(g_2^{a_j x_1}, g_1^{\frac{q_x(0)}{a_j}}\cdot f_1\left(A_j,t_m\right)^{h}\right)\cdot\hat{e}\left(g_2^{a_j h}, f_1\left(A_j,t_m\right)^{x_1}\right)^{-1}\\
&= X\cdot Y^{x_1}\cdot\prod_{j\in\gamma_j}\hat{e}\left(g_2^{a_j x_1}, g_1^{\frac{q_x(0)}{a_j}}\right)^{-1} = X\cdot Y^{x_1}\cdot\prod_{j\in\gamma_j}\hat{e}(g_2,g_1)^{-q_x(0)x_1}\\
&= X\cdot Y^{x_1}\cdot Y^{-x_1} = X
\end{aligned}
$$

Equipped with $C_2^{'}$ and X, a delegatee can recovers M by calculating (8) since:

$$
\frac{C_0}{C_2^{'(f_2(X))^{-1}}} = \frac{M\cdot Y^{s}}{Y^{f_2(X)s(f_2(X))^{-1}}} = M \qquad (12)
$$

The proof of *Test* is demonstrated in (13):

$$
\begin{aligned}
&\prod_{j\in\gamma_j}\hat{e}\left(IN_{2,j}, TR_{1,j}\right)\cdot\hat{e}\left(IN_{3,j}, TR_{3,j}\right)^{-1}\cdot\hat{e}\left(IN_1, TR_{2,j}\right)^{-1} \qquad (13)\\
&= \prod_{j\in\gamma_j}\hat{e}\left(g_2^{a_j x_2}, \left(g_1^{\frac{q_x(0)}{a_j}}\cdot f_1\left(A_j,t_m\right)^{h}\cdot g_1^{l}\right)^{f_2(w)}\right)\cdot\hat{e}\\
&\left(f_1\left(A_j,t_m\right)^{x_2}, g_2^{ha_j f_2(w)}\right)^{-1}\cdot\hat{e}\left(g_1^{x_2}, g_2^{a_j f_2(w) l}\right)^{-1}\\
&= \prod_{j\in\gamma_j}\hat{e}\left(g_2^{a_j x_2}, g_1^{\frac{q_x(0)}{a_j}f_2(w)}\right) = \prod_{j\in\gamma_j}\hat{e}(g_2,g_1)^{f_2(w)q_x(0)x_2}\\
&= \hat{e}(g_2,g_1)^{f_2(w)yx_2} = IN_0
\end{aligned}
$$

5.2 Confidentiality and keyword semantic security:

Theorem 1: The proposed scheme is confidential in the selective model if DBDH assumption holds.

- Proof: If an *Adversary* can break the confidentiality in our scheme with non-negligible advantage ε, then a simulator can be constructed to solve the DBDH problem with $\frac{\varepsilon}{2}$.

Theorem 2: The proposed scheme is keyword semantic secure in the selective model if DBDH assumption holds.

- Proof: If an *Adversary* can break the keyword semantic security in our scheme with non-negligible advantage ε, then a simulator can be constructed to solve the DBDH problem with $\frac{\varepsilon}{2}$.

The methods we adopt to conduct the proof of theorem 1 and theorem 2 had been covered in detail in our previous work [22], and not repeated in this paper.

5.3 Collusion resistance

Since there exist some malicious delegatees and the server is considered to be semi-trusted, effective measures should be taken to prevent collusion attack which may happen during the process of data sharing. In this paper we satisfy this significant security demand by introducing two generators in the cyclic group as well as other secret parameters in the re-encryption keys and search indexes. In particularly, if a malicious delegatee colludes with sever and merge their private information together, they can obtain the *rk*, *IN*, *TR* and *SK* of the delegatee and their purpose is to computes *SK* of the delegator. Note that among these parameters only $rk(\{rk_{1,\ i}, rk_{2,\ i}, rk_{3,\ i}, C_1^{'}\})$ contains the secrets of delegator's private key. From the process of decryption we can figure out that even equipped with *rk* and *SK* of the delegatee, still *SK* of delegator cannot be calculated since the value of $g_1^{\ k}$ remains unknown, thus our scheme meets the security demand of collusion attack.

6 Conclusion

This paper proposes an ABDR-PRE scheme which allows a delegator generates search indexes and re-encryption keys over the target ciphertexts to be re-encrypted. It meets the security requirements of confidentiality, keyword semantic security and resistance of collusion attack. The high security level and multiple functions makes it an applicable scheme to provide efficient data sharing and retrieval in data outsourcing scenarios.

Acknowledgements This research is supported by the National Natural Science Foundation of China (61373135, 61672299).

Compliance with Ethical Standards

Competing Interest The authors declare that they have no competing financial interests.

References

1. Li J, Liu Z, Chen X, Tan X, Wong DS (2015) L-EncDB: A Lightweight Framework for Privacy-Preserving Data Queries in Cloud Computing. Knowl-Based Syst 79:18–26
2. Huang Z, Liu S, Mao X, Chen K, Li J (2017) Insight of the Protection for Data Security under Selective Opening Attacks. Inf Sci 412–413:223–241
3. Bhuiyan MZA, Wu J, Wang G, Chen Z, Chen J, Wang T (April 2017) Quality-Guaranteed Event-Sensitive Data Collection and Monitoring in Vibration Sensor Networks. IEEE Transactions on Industrial Informatics 13(2):572–583
4. Bhuiyan MZA, Wu J, Wang G, Cao J (2016) Sensing and Decision-making in Cyber-Physical Systems: The Case of Structural Health Monitoring. IEEE Transactions on Industrial Informatics 12(6): 2103–2114
5. Liu X, Choo K-KR, Deng RH, Lu R, Weng J (2018) Efficient and Privacy-Preserving Outsourced Computation of Rational Numbers. IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) 15(1):27–39. https://doi.org/10.1109/TDSC.2016.2536601
6. Liu X, Deng RH, Choo K-KR (2018) Privacy-Preserving Outsourced Calculation Toolkit in the Cloud. IEEE Transactions on Dependable and Secure Computing (IEEE TDSC). https://doi.org/10.1109/TDSC.2018.2816656
7. Hong H, Sun Z, Liu X (2017) Provably secure attribute based signcryption with delegated computation and efficient key updating. KSII Transactions on Internet and Information Systems 11(5):2646–2659
8. Liu Z, Huang Y, Li J (2018) DivORAM: Towards a Practical Oblivious RAM with Variable Block Size. Inf Sci 447:1–11
9. Xu J, Wei L, Yu Z (April 2018) Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures. Volume 107(1):113–124
10. Sahai A, Waters B (2005) Fuzzy identity-based encryption. Advances in Cryptology-EUROCRYPT:457–473
11. Goyal Y, Pandey O, Sahai A, et al (2006) Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications. Security 89-98
12. Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy 2007:321–334
13. Waters B (2011) Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Public Key Cryptography-PKC 2011:53–70
14. Li LF, Chen XW, Jiang H et al (2016) P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds. 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 575-580
15. Reedy BE, Ramu GH (2016) A Secure Framework for Ensuring EHR's Integrity Using Fine-Grained Auditing and CP-ABE. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS): 85-89
16. Liu Z, Wong DS (2015) Practical Ciphertext-Policy Attribute-Based Encryption: Traitor Tracing, Revocation, and Large Universe". Volume 9092 of the series Lecture Notes in Computer Science, Applied Cryptography and Network Security 127-146
17. Yang K, Jia XH, Ren K et al (2013) DAC-MACS: Effective data access control for multi-authority cloud storage systems. IEEE Transactions on Information Forensics and Security, Information Security 8(11):87–99
18. Padhya M, Jinwala D (2014) A Novel Approach for Searchable CP-ABE with Hidden Ciphertext-Policy. Volume 8880 of the series Lecture Notes in Computer Science, Information Systems Security 167-184
19. Miyaji A, Phuong VX (2012) Constant-ciphertext-size dual policy attribute based encryption. Volume 7672 of the series Lecture Notes in Computer Science, Cyberspace Safety and Security 400-413
20. Cheng Y, Wang ZY (2013) Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage. Journal of Zhejiang University SCIENCE C 14(2):85–97
21. Qiu S, Liu JQ, Shi YF et al (2017) Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. Volume 8880 of the series Lecture Notes in Computer Science. Inf Syst Secur 60:052105
22. Hong H, Sun Z (2018) Achieving secure data access control and efficient key updating in mobile multimedia sensor networks. Multimedia Tools and Applications 77(4):4477–4490
23. Hong H, Sun Z (2016) High efficient key-insulated attribute based encryption scheme without bilinear pairing operations. Springerplus 5
24. Lin Q, Li J, Huang Z, Chen W, Shen J A short linearly homomorphic proxy signature scheme. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2809684