A Ciphertext Policy through Deniable Attribute Based Encryption for Cloud Storage

[1]Shrawan Kumar Purve, [2]Abhijeet Katkar,[3]Swapnil Kamble,[4]Sukeshani Bhagat, [5]Monali Modankar

[1]Asst.Prof, Dept. ofCSE,SSCET, Bhadrawati, E-mail : shravankumar.purve@gmail.com
[2]Final year, Dept. of CSE,SSCET, Bhadrawati, E-mail :abhijeetkatkar159@gmail.com
[3]Final year, Dept. of CSE,SSCET, Bhadrawati, E-mail :kambleswapnil91@gmail.com
[4]Final year, Dept. of CSE,SSCET,Bhadrawati, E-mail :sukeshnibhagat764@gmail.com
[5]Final year, Dept. of CSE,SSCET, Bhadrawati, E-mail :monali143modankar@gmail.com

***Abstract*:**Cloud storage is a place where the large amount of data can be stored. In a digital era many Hi-tech multinational companies are using cloud to store their data not every companies can afford a database to store the data so they hires an space in someone's cloud to store their important data. As cloud is used to store the data then security is an important issue. Security to secure the data owners data and for security we are introducing the Deniable Cipher text- attribute based encryption.Many of the cloud security schemes are failed coz it was a third party handling to keep track of the data. In our concept we use directly interaction between cloud customer, Key Distribution Center (KDC) and the End User, which don't need a third party handling to maintain the data, it minimizes the time complexity. Most of the schemes are failed due to third party handlingi.e. to maintain data record manually but, we are setting the data free, we are not maintaining the data manually we are making it Audit Free i.e. automatic maintenance of data. The deniability of features makes coercers unauthorized. If an coercers forcefully tries to download the data without an authority and the permission he/she will we provided an fake data so that our data will be secured and coercers will also be satisfied with some similar data.
In this paper we describe Attribute Bases Encryption, which performs the operation for secure stored data such as, Fine-grained access control and deniable encryption. The fine grained access control provides the secret key to cloud system

Keywords: *Deniable Encryption, Composite order Bilinear Group, Attribute-Based Encryption, Cloud Storage.*

*****

1. INTRODUCTION

Cloud storage is a type of information stockpiling where the computerized information is put away in consistent pools, the physical stockpiling traverse different servers (and frequently areas), and the physical environment is regularly claimed and taken care of by a facilitating association. These distributed storage suppliers are responsible for keeping the information accessible and available, and the physical environment ensured and running.Considering the shared property of the cloud information, attribute-based encryption (ABE) is viewed as a standout **amongst** the most reasonable encryption plans for distributed storage. There are various ABE plans that have been proposed.This idea originates from a unique sort of encryption plan called deniable encryption, initially proposed in. Deniable encryption includes senders and recipients making persuading fake proof of fashioned information in cipher texts with the end goal that outside coercers are satisfied.In this paper, we introduce our plan for another distributed storage encryption conspire that empowers distributed storage suppliers to make persuading fake client privileged insights to secure client protection. Since coercers can't confess if acquired mysteries are valid or not, the distributed storage suppliers guarantee that client security is still safely ensured. In this work, we portray a deniable ABE plot for distributed storage administrations. We make utilization of ABE attributes for securing put away information with a fine-grained get to control component and deniable encryption to avert outside inspecting. Our plan is based on Waters cipher text policy-attribute based encryption (CP-ABE) plot. We upgrade the Waters plot from prime request bilinear gatherings to Composite request bilinear gatherings. By the subgroup choice issue suspicion, our plan empowers clients to have the capacity to give fake insider facts that appear to be genuine to outside coercers. A focal security highlight of Attribute-Based Encryption is arrangement resistance: A challenger that grips numerous keys should just be able to get to information if no less than one individual key awards get to. The point picking this attribute-based encryption is that as more responsive, information is shared and put away by outsider locales on the Internet, there will be a need to scramble information put away at these destinations. One disservice of scrambling information is that it can be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). To beat this impediment we utilized another

cryptosystem for fine-grained sharing of encoded information that we call Key Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher text are marked with sets of attributes and private keys are connected with get to structures that control which cipher text by this the client can without much of a stretch ready to decode the information which was scrambled. The materialness of this development is to share the review log data and communicate encryption **furthermore** underpins designation of private keys which incorporates the Hierarchical Identity-Based Encryption. These Encryption plans guaranteeing that distributed storage specialist co-ops or trusted outsiders taking care of key administration are trusted and can't be hacked.

1.1 Previous Work on ABE

AmitSahai and Brent Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. That is, only those who match the owner's conditions can successfully decrypt stored data. We note here that ABE is encryption for privileges, not for users. This makes ABE a very useful tool for cloud storage services since data sharing is **an** important feature for such services. There are so many cloud storage users that it is impractical for data owners to encrypt their data by pair wise keys.

There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE). The difference between these two lies in policy checking. KP-ABE is an ABE in which the policy is embedded in the user secret key and the attribute set is embedded in the cipher text. Conversely, CP-ABE embeds the policy into the cipher text and the user secret has the attribute set. Goyal et al. proposed **the** first KP-ABE. They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bettencourt et al. proposed the first CP-ABE. This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the cipher text. The first fully expressive CP-ABE was proposed by Waters, which used Linear Secret Sharing Schemes (LSSS) to build a cipher text policy. Lewko et al. enhanced the Waters scheme to a fully secure CP-ABE, though with some efficiency loss. Recently, Attrapadung et al. constructed a CP-ABE with a constant-size cipher text in and Tysowski et al. designed their CP-ABE scheme for resource-constrained users.

1.2 Previous Work on Deniable Encryption

Considering the cloud storage scenario, we focus our efforts on the deniable public key encryption scheme.There are some important deniable public key encryption schemes2. Canetti et al. used translucent sets to construct deniable encryption .A translucent set is a set containing a trapdoor subset. It is easy to randomly pick an element from the universal set or from the subset; however, without the trapdoor, it is difficult to determine if a given element belongs to the subset. Canetti et al. showed that any trapdoor permutation can be used to construct the translucent set. To build a deniable public key encryption scheme from a translucent set, the translucent set is the public key and the trapdoor is the private key. The translucent set is used to represent one encrypted bit. Elements in the subset are represented by 1 whereas other non-subset elements are represented by 0. The sender can encrypt 1 by sending an element in the subset, but can claim the element is chosen from the universal set (i.e., 0). The above is a basic sender-deniable scheme. Canetti et al.

The translucent set is used to represent one encrypted bit. When sending an encrypted bit, the sender will send a set of encrypted data which may be normally encrypted or oblivious. Therefore, the sender can claim some sent messages are **oblivious** while actually they are not. The idea can be applied to the receiver side such that the scheme is a bi-deniable scheme. In Gasti et al. proposed another deniable scheme in which one public **private** key pair is set up for each user while there are actually two pairs. The sender can send a true message encrypted by one key with a fake message encrypted by the other key.

Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, e**n**crypted data are assumed to be known and storage providers are requested to release user secrets. Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE). Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bettencourt et al. proposed the first CP-ABE. This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the cipher text.

2. PROPOSED SYSTEM

We make use of Composite order bilinear groups to construct the multidimensional space. We also use chameleon hash functions to make both true **and** fake messages **convincing**. Our deniable ABE has the advantages described below over previous deniable encryption schemes.In this work, we construct a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers

are just regarded as receivers in other deniable schemes. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to **predetermined** fake data. The information defining the dimensions is kept secret. There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE). Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bettencourt et al. proposed the first CP-ABE. This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the cipher text.

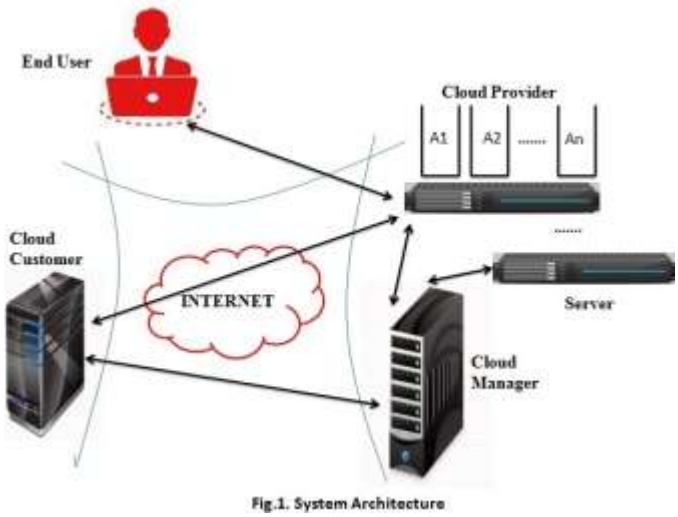

Fig.1. System Architecture

2.1 Scheme Description

Most deniable public key schemes are bitwise, which means these schemes are able to process one bit a time. Hence, bitwise deniable encryption schemes are incompetent for real use, especially in the cloud storage service case. To resolve this problem, considered a hybrid encryption scheme that concurrently uses symmetric and **asymmetric** encryption they use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. Mainly deniable encryption schemes have decryption error problems. These errors come from the considered decryption mechanisms.So no one can pick up the control key of a repudiated file in future. Due to this reason we can say the file is certainly erased. To get well the file, the user must ask for the key controller to fabricate the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is confirmed by means of an attribute connected with the file.

• **Block wise Deniable ABE**. Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. To solve this problem, O'Neil et al. designed a hybrid encryption scheme that simultaneously uses symmetric and asymmetric encryption.ABE scheme by replacing **prime** order groups with composite order groups. Since the base ABE scheme can encrypt one block each time, our deniable CPABE is certainly a block wise deniable encryption scheme. Though the bilinear operation for the Composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from composite order groups to prime order groups for better computational performance.

• **Consistent Environment.** Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility.

In this work, we build a consistent environment for our deniable encryption scheme. By consistent environment, we mean that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this **environment3**, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal cipher texts correctly.

• **Deterministic Decryption.** Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms. For example, Canetti et al. uses the subset decision mechanism for decryption. The receiver determines the decrypted message according to the subset **decision** result. Decryption is correct if and only if the correct part overwhelms the false part. Otherwise, the receiver will get the error result. The concept of our deniable scheme is different than these schemes described.

Advantages of Proposed System:

 Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. Instead, we adopt the idea proposed with some improvements. We construct our deniable encryption scheme through a **multidimensional** space. All data are encrypted into the multidimensional space.

 Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The

information defining the dimensions is kept secret. We make use of Composite order bilinear groups to construct the multidimensional space. We also use chameleon hash functions to make both true and fake messages convincing.

 In this work, we build a consistent environment for our deniable encryption scheme. By consistent environment, we mean that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal cipher texts correctly.

3. ORGANIZATION

In additional to this introductory section, we introduce preliminaries used in this paper we formally define deniable CP-ABE and its properties. Also we show how to set up a basic deniable CPABE scheme and prove security, deniability and other features of our scheme.

3.1 Chameleon Hash

The idea behind the chameleon hash scheme was first Introduced. Just like other common secure hash functions, a chameleon hash scheme has two key properties, namely collision resistance and semantic security. Further, a chameleon hash scheme also provides collision forgery with a predetermined **trapdoor**. The input of a chameleon hash includes two parts, one being input message m and the other random string r. The random string r is used to provide a chance to adapt the message for the hash value.

4. DEFINITIONS

4.1 Deniable CP-ABE Scheme:

Deniable encryption schemes may have different properties and we provide an **introduction** to many of these properties below.

•ad hoc deniability vs. plan-ahead deniability: The former can generate a fake message (from the entire message space) when coerced, whereas the **latter** requires a predetermined fake message for encryption. Undoubtedly, all bitwise encryption schemes are adhoc.

• Sender-, receiver-, and bi-deniability: The prefix here in each case implies the role that can fool the coercer with convincing fake evidence. In senderdeniable encryption schemes and **receiver**-deniable schemes, it is assumed that the other entity cannot be coerced. Bi-deniability means both sender and receiver can generate fake evidence to pass thirdparty coercion.

• Full deniability vs. multi-distributional deniability: A fully deniable encryption scheme is one in whichrandom for encryption composite order group. The decryption algorithm in our scheme is still deterministic; therefore, there is no decryption errors using our scheme.

4.2 Security Proof**:** To prove that our deniable encryption scheme is secure requires this scheme to be a valid encryption scheme. For a multi-distributional deniable encryption scheme, it is only necessary to prove the security from the normal algorithm set. That is, we only need to prove the security of a scheme composed of the following four algorithms Setup, KeyGen, Enc, and Dec.

• Setup(1λ) → (PP,MSK): This algorithm takes security parameter λ as input and returns public parameter PP and system **master key** MSK.

• KeyGen(MSK,S) → SK: Given set of attributes S and MSK, this algorithm outputs private key SK.

• Enc(PP,M,A) → C: This encryption algorithm takes as input public parameter PP, message M, and LSSS access structure A = (M,ρ) **over** the universe of attributes. This algorithm encrypts M and outputs a cipher text C, which can be decrypted by those who possess an attribute set that satisfies access structure A. Note that A is contained in C.

• Dec(PP,SK,C) → {M,⊥}: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and ciphertext C with its access structure A. If S satisfies A, then this algorithm returns M; otherwise, this algorithm returns ⊥.

• OpenEnc(PP,C,M) → PE: This algorithm is for the sender to release encryption proof PE for (M,C).

• OpenDec(PP,SK,C,M) → PD: This algorithm is for the receiver to release decryption proof PD for (M,C).

• Verify(PP,C,M,PE,PD) → {T,F}: This algorithm is used to verify the correctness of PE and PD.

•DenSetup(1λ) → (PP,MSK,PK): This algorithm takes security parameter λ as input and returns public parameters PP, system master key MSK, and system public key PK. PK is known by all system users and is kept secret to outsiders.

• DenKeyGen(MSK,S) → (SK,FK): Given set of attributes S and MSK, this algorithm outputs private key SK as well as FK for the user, where FK will be used for generating fake proof later.

• DenEnc(PP,PK,M,M′,A) → C′: Aside from the inputs of the normal encryption algorithm, this deniable encryption algorithm needs public key PK and fake message M′. The output ciphertext must be indistinguishable from the output of Enc.

• DenOpenEnc(PP,C′,M′) → P′ E: This algorithm is for the sender to release encryption proof P′ E for fake message M′.

The output must be indistinguishable from the result of OpenEnc and must pass the Verify algorithm.

• DenOpenDec(PP,SK,FK,C′,M′) → P′ D: This algorithm is for the receiver to release decryption proof P′ D for fake message M′. The output must be indistinguishable from the result of OpenDec and must pass the Verify algorithm.

4.3 Deniability Proof: To prove the deniability of our CP-ABE scheme, we must show (M,C, PE, PD) and (M′,C′, P′ E, P′ D) are indistinguishable. Since M,C,PE,PD are pairwise independent because of the security property, weneed only show the indistinguishability between C and C′, PE and P′ E , and PD and P′ D . Lemma 1: Under the general subgroup decision assumption, normal cipher text C and deniable cipher text C′ are indistinguishable. The deniable CP-ABE is deniable receiver proof consistent if a deniable receiver proof is convincing even when considering all cipher texts in the system. That is, given set of cipher texts C, including normally encrypted cipher texts and deniably encrypted cipher texts, normal proof PD and deniable proof P′ D, there is no PPT algorithm A for which

$$Adv_A := |P[A(C,PD) = 1] - P[A(C,P' D) = 1]|$$

is non-negligible.

4.4 Decryption Errors: In section 1, we described why most deniable schemes may cause decryption errors. Most of these schemes claim their decryption error rates are small or negligible, but they cannot ensure that there are no errors whatsoever in their schemes. In our scheme, a receiver uses a one-way function with a signature to obtain the true message. Both the one-way function and the signature are generated by the sender.

5. PERFORMANCEEVALUATIONS

In this section, we evaluate the performance of our idea by implementing two deniable schemes: the composite order scheme and the prime order simulation scheme. We compare them with the Waters scheme. We use the Pairing Based Cryptography (PBC) library for cryptographic operations. Our experiments focus on one block encryption/decryption. A large file can be divided into multiple blocks, and all blocks can be protected by one secret s. Because GT multiplication and H are lightweight operations, we use one-block encryption/decryption to evaluate the performance. Our experiments focus on encryption and decryption performance. The Setup and KeyGen performance are skipped because these two algorithms are not time critical. The four Open algorithms are low-cost algorithmsbecause these algorithms only return existing information. The cost of Verify algorithm is equal to that of Dec. Note that we do not distinguish deniable encryption from normal encryption; their numbers of arithmetic operations and pairing operations are equal, and therefore the normal one and the deniable one will have similar performance. In our design, the encryption cost and the decryption cost depend on required attribute numbers. For convenience, we make all attributes mandatory as our cryptographic policy. We run the experiments with different attribute numbers, from 10 to 1000. Our experiments focus on one block encryption/decryption.

6. RESULT

Our cloud storage encryption schemes are proposed to protect data from those who do not have access i.e. coercers. We are assuring that cloud security is secure and can't be hacked, if any fake user try's to download the data then he will be provided an fake data so that our data will be safe and fake user will also be satisfied. Cloud computing basically needs resources i.e. software and the hardware and the service is given through the means of internet. We don't use public keys. We are implementing multiple encryptions without any system updates. Our four import modules are Key Distribution center(KDC) KDC provides the accessibility of files to users. Initially User will request for a secret key pair for the selected file. Data Owner New data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model.Cloud server User is able to decrypt the cipher text. User ModuleAuser can obtain the true message with a valid secret key from KDC, regardless of whether the cipher text is normally encrypted or deniably encrypted. Search over files The proposed scheme should allow search over encrypted files which would be encrypted and stored in the cloud.

Thus our project is secured and maintenance free.

7. CONCLUSIONS

In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism.A deniable CP-ABE scheme is an audit-free cloud storage service. The deniability feature makes force invalid, and the Attribute Based Encryption belongings guarantee secure cloud data sharing with a fine-grained access control method. This scheme presents a likely way to struggle next to dissipated intervention with the right of privacy. Not only the above can this scheme be formed to guard cloud user privacy with high computational performance.

Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We

hope more schemes can be created to protect cloud user privacy.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[3] J. Bettencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70.

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and cipher text delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.

[7] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.

[8] Wired. (2014) Spam suspect uses Google docs; fbihappy.[Online].Available:http://www.wired.com/2010/04/cl oud-warrant/

[9] Wikipedia.(2014)Global surveillance disclosures (2013present).[Online].Available:http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)

[10] (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden [12] (2014) Lavabit.[Online]. Available: http://en.wikipedia. org/wiki/Lavabit.

[11] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in Eurocrypt, 2010, pp. 44–61.

[12] A. B. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in Eurocrypt, 2012, pp. 318–335.

[13] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of technology, 1996.

[14] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on cipher texts," in TCC, 2005, pp. 325–341.

[15] H. Krawczyk and T. Rabin, "Chameleon signatures," in NDSS, 2000.

[16] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short cipher texts and private keys," in Eurocrypt, 2006, pp. 573–592.

[17] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Eurocrypt, 2008, pp. 146–162.

[18] S. Meiklejohn, H. Shacham, and D. M. Freeman, "Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures," in Asiacrypt, 2010, pp. 519–538.

[19] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-cipher text security from identity-based encryption," SIAM J. Comput., vol. 36, no. 5, pp. 1301–1328, 2007.

[20] K. Liang, L. Fang, D. S. Wong, and W. Susilo, "A cipher textpolicy attribute-based proxy re-encryption with chosen-cipher text security," IACR Cryptology ePrint Archive, vol. 2013, p. 236, 2013.