Privacy-Preserving Cipher Text Multi-Sharing Management for Big Data Storage

V. Srikanth[1], J. Venkata Gopal[2]

[1]PG Student, Dept. of Computer Science and Engineering, Brahmaiah College of Engineering, Nellore, India

[2]Associate Professor & HoD, Dept. of Computer Science and Engg., Brahmaiah College of Engg., Nellore, India

***Abstract*: The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients. Furthermore, the paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.**

***Keywords*: Privacy, anonymity, proxy re-encryption, big data.**

1. Introduction

To date many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever.

A basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypts the data under the public key of receiver such that no one except the valid recipient can gain access to the data. Nevertheless, this does not satisfy all the requirements of users in the scenario of big data storage.

Consider the following scenario. We suppose a hospital stores its patients' medical records in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. By using some traditional PKE, Identity-Based Encryption (IBE), or Attribute-Based Encryption (ABE), the confidentiality of the record can be protected effectively.

By trivially employing traditional encryption mechanisms (to guarantee the confidentiality of medical record), nevertheless, we cannot prevent some sensitive personal information from being leaked to the cloud server but also the public. This is because traditional encryption systems do not consider the anonymity of a ciphertext sender/receiver. Accordingly, someone, could be anyone with capability of obtaining a ciphertext (e.g. cloud server), may know whose public key the ciphertext is encrypted under, namely who is the owner of the ciphertext, such that the patient associated with the ciphertext can be easily identified. Similarly, the recipient/destination of the ciphertext, e.g., Cardiology Dept., can be known from the ciphertext without any difficulty as well. This seriously disgraces the privacy of patient.

Moreover, a patient might be transferred to more than one medical department in different treatment phases. The corresponding medical record then needs to be converted to the ciphertexts corresponding to various receivers so as to be shared among the departments. Therefore, the update of ciphertext recipient is desirable. Precisely speaking, a fine-grained ciphertext update for receivers is necessary in the sense that a ciphertext can be conditionally shared with others. The medical record owner, e.g., the patient, has rights to decide who can gain access to the record, and which kinds of data are allowed for access. For example, the patient can choose to specify that only the medical record described with "teeth" can be read by a dentist. This fine-grained control prevents a data sharing mechanism from being limited to the "all-or-nothing" share mode.

This research work aims to solve the above problems. To preserve anonymity, some well-known encryption mechanisms are proposed in the literature, such as anonymous IBE [8]. By employing these primitives, the source and the destination of data can be protected privately. However, the primitives cannot support the update of ciphertext receiver.

There are some naive approaches to update ciphertext's recipient. For instance, data owner can employ the decrypt-then-re-encrypt mode. Nonetheless, this is applicable to the scenario where there is only a small amount of data. If the encrypted data is either a group of sequences of genome information or a network audit log, the decryption and re-encryption might be time consumed and computation costly. Moreover, this mode also suffers from a limitation that the data owner has to be on-line all the time. Alternatively, a fully trusted third party with knowledge of the decryption key of the data owner may be delegated to handle the task. Nevertheless, this strongly relies on the fully trust of the party. Besides, the anonymity of the ciphertext receiver cannot be achieved as the party needs to know the information of recipient to proceed the re-encryption. Therefore, both of the approaches do not scale well in practice.

Introduced by Mambo and Okamoto and further de-fined in [5], Proxy Re-Encryption (PRE) is proposed to tackle the dilemma of data sharing. It allows a semi-trusted party, called proxy, to transform a ciphertext intended for a user into a ciphertext of the same message intended for another user without leaking knowledge of either the decryption keys or the message. The workload of data owner is now transferred to the proxy, and the "on-line all the time" requirement is unnecessary.

This work concentrates on the identity-based cryptographic setting. To employ PRE in the IBE setting, [17] defined the notion of Identity-Based Proxy Re-Encryption (IBPRE), which offers a practical solution for access control in networked file storage [17], and secure email with IBE [17]. To capture privacy-preserving property and ciphertext's recipient update simultaneously, proposed an anonymous IBPRE system, which is CCA security in the Random Oracle Model (ROM).

The valuable work introduces the first anonymous IBPRE in the literature and meanwhile, it leaves us interest-ing and meaningful open problems. The work only supports one-time ciphertext receiver update, while multiple receivers update is desirable in practice. On the other hand, the work provides an "all-or-nothing" share mode that limits the flexi-bility of data sharing.

A. *Our contributions*

In this paper, we aim to propose a ciphertext sharing mechanism with the following properties:

Anonymity: given a ciphertext, no one knows the identity information of sender and receiver.

Multiple receiver-update: given a ciphertext, the receiver of the ciphertext can be updated in multiple times. In this paper, we refer to this property as "multi-hop".

Conditional sharing: a ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied.

Achievements: We investigate a new notion, AMH-IBCPRE. We formalize the definition and security model by incorporating the definitions. In the security model, we allow the corrupted users to be adaptively chosen by an adversary, while the adversary must output the challenge identity at the outset of security game. Moreover, we define four security models for different practical purposes.

The security model of MH-IBCPRE is the basic one, in which a challenger plays the game with the adversary to launch Chosen-Ciphertext Attacks (CCA) to the original ciphertext and re-encrypted ciphertext in order to solve a hard problem.

We also consider the case where a proxy colludes with delegatee to compromise the underlying message and the secret key of delegator. Here, the protection of the message is very difficult to achieve as the delegatee can always decrypt the corresponding ciphertext for the proxy. The secret key of the delegator, however, is possible to be secured. For the definition of collusion attacks model, we allow an adversary to acquire all re-encryption keys, and the adversary wins the game if it outputs a valid secret key of an uncorrupted user. We note that our definition is in the selective model in which the adversary has to output a target identity at the outset of the game.

As to the security model of anonymity, it is complicated in the sense that we categorize the game into two sub-games: one is the anonymity for delegator (i.e. given the original ciphertext an adversary cannot output the identity of delegator), the other is the anonymity of re-encryption key (i.e. an adversary cannot distinguish a valid re-encryption key from a random one belonging to re-encryption key space).

We next propose a concrete construction for unidirec-tional AMH-IBCPRE, in which it achieves multiple cipher-text receiver update, conditional data sharing, anonymity and collusion-safe (i.e. holding against collusion attacks) simulta-neously in asymmetric bilinear group. Note the functionality of our system is generally described in Fig 1. We state that the new primitive is applicable to many real-world applications, such as secure email forwarding, electronic encrypted data sharing, where both anonymity and flexible encrypted data sharing are needed. We also show that the scheme is CCA-secure in the standard model under the decisional P -Bilinear Diffie-Hellman assumption. To the best of our knowledge, our system is the first of its kind in the literature.

B. *Related work*

Following the concept of delegation of decryption rights introduced by Mambo and Okamoto [26], Blaze et al. [5] formalized the concept of PRE, and proposed a seminal bidirectional PRE scheme. Afterwards, many PRE schemes have been proposed, such as [2], [3], [11], [18], [19], [20]. Employing traditional PRE in the context of IBE, Green and Ateniese [17] initially introduced the notion of IBPRE, and proposed two unidirectional IBPRE schemes in the ROM: one is CPA secure and the other holds against CCA. Later on, two CPA-secure IBE-PRE schemes (in the types of PKE-IBE and IBE-IBE) have been proposed. Afterwards, some IBPRE systems have been proposed for various requirements. In the multiple ciphertext receiver update1 scenario, Green and Ateniese [17] proposed the first MH-IBPRE scheme with CPA security. Later on, a RCCA-secure MH-IBPRE scheme. We refer to multiple ciphertext receiver update to a notion called

Multi-Hop (MH) in this paper.

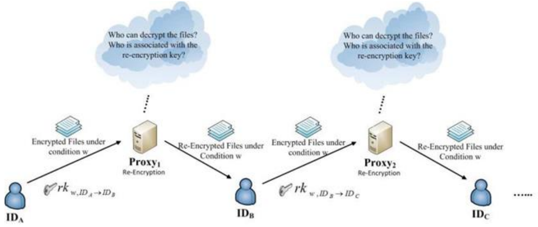
Who can decrypt the files?
Who is associated with the re-encryption key?
Who can decrypt the files?
Who is associated with the re-encryption key?
Encrypted Files under condition w
Proxy$_1$
Re-Encryption
Re-Encrypted Files under Condition w
Encrypted Files under condition w
Proxy$_2$
Re-Encryption
Re-Encrypted Files under Condition w
$rk_{w,ID_A \to ID_B}$
$rk_{w,ID_B \to ID_C}$
ID$_A$
ID$_B$
ID$_C$
......

Fig. 1. Anonymous multi-hop identity-based conditional proxy re-encryption

without random oracles was proposed by Chu and Tzeng [12]. These schemes, however, are not collusion-safe. To solve the problem, Shao and Cao proposed a CCA-secure MH-IBPRE in the standard model with collusion-safe property. To hide the information leaked from re-encryption key, Ateniese et al. [1] defined the notion of key-privacy (i.e. an adversary cannot identify delegator and delegatee even given re-encryption key). Later on, Shao et al. revised the security model introduced in [1].

To prevent a ciphertext from being traced, Emura et al. [15] proposed a unidirectional IBPRE scheme in which an adversary cannot identify the source from the destination ciphertext. To ensure the privacy of both delegator and delegatee, Shao et al. proposed the first Anonymous PRE (ANO-PRE) system. The system guarantees that an adversary cannot identify the recipient of original and re-encrypted ciphertext even given the corresponding re-encryption key. In 2012, Shao also proposed the first anonymous IBPRE with CCA security in the ROM.

In the context of IBE/ABE, some well-known systems supporting anonymity that have been proposed, such as [8], [9], [16]. Leveraging them may partially fulfill our goals. However, we need to focus on the combination of anonymity and ciphertext update properties. Therefore, the aforementioned systems are not taken in comparison below.

Here, we compare our work with some related systems, and summarize the comparison of properties in Table I. While multiple ciphertext receiver update (denoting as M.U.), conditional (data) share, collusion resistance (denoting as C.R.), anonymity, and without random oracle (denoting as W.R.O.), have all five been partially achieved by previous schemes, there is no effective CCA-secure proposal that achieves all properties simultaneously in the standard model. This paper, for the first time, fills the gap.

2. System definition and threat models

A. System definition

Definition 1: A unidirectional Multi-Hop Identity-Based Conditional Proxy Re-Encryption (MH-IBCPRE) scheme consists of the following algorithms:

1) $(mpk, msk) \leftarrow Setup(1^k)$: on input a security parameter k, output a master public key *mpk* and a master secret key *msk*. For simplicity, we omit *mpk* in the expression of the following algorithms.
2) $sk_{ID} \leftarrow Keytten(msk, ID)$: on input *msk*, and an identity $ID \in \{0, 1\}*$, output a secret key sk_{ID}.
3) $rk_{w,ID}i{\to}ID$it ~~Re~~$Keytten(ID_i, sk_{ID}i$, ID_it , w): on input a delegator's identity ID_i and the correspond- ing secret key $sk_{ID}i$, a delegatee's identity ID_it , and a condition $w \in \{0, 1\}*$, output a re-encryption key $rk_{w,ID}i{\to}ID$it from ID_i to ID_it under condition w.
4) $C_{1,ID}i,w \leftarrow Enc(ID_i, w, m)$: on input an identity ID_i, a condition w and a message m, output a 1-level ciphertext $C_{1,ID}i,w$ under identity ID_i and w.
5) Cl+1,IDit ,$w \leftarrow ReEnc(rkw,ID_i{\to}ID$it , Cl,ID_i,w): on input $rk_{w,ID}i{\to}ID$it , and an l-level ciphertext $C_{l,ID}i,w$ under identity ID_i and w, output an $(l + 1)$-level ciphertext $C_{l+1,ID}$it ,w under identity ID_it and w or $\perp$ for failure, where $l \geq 1$, l N∈.
6) $m \leftarrow Dec(sk_{ID}i$, $C_{l,ID}i,w$): on input $sk_{ID}i$, and an l-level ciphertext $C_{l,ID}i,w$ under identity ID_i and w, output a message m or $\perp$ for failure, where $l \geq 1$, $l \in$ N.

B. Threat models

We define four models in terms of the selective condition and selective identity chosen ciphertext security (IND-sCon-sID-CCA), collusion resistance, the anonymity of the original ciphertext and anonymity of the re-encryption key in this section. Before proceeding, we define some notations.

Delegation Chain. There is a set of re-encryption keys RK = f^{rk}w;ID$_{i1}$!ID$_{i2}$; :::; ^{rk}w;ID$_{il}$ $_1$!ID$_{il}$ g under the same condition w, for any re-encryption key ^{rk}w;ID$_{ij}$!ID$_{ij+1}$ in RK, ^{ID}i$_j$ 6= ^{ID}i$_{j+1}$. We say that there exists a delegation chain under w from identity ID$_{i1}$ to identity ID$_{il}$, denoted as wjID$_{i1}$! ::: ! ID$_{il}$. Note this delegation chain includes the case where ID$_{i1}$ = ID$_{il}$. Besides, we use wjID to indicate a ciphertext under w and ID, and for a single identity ID we use ? jID to denote it.

Uncorrupted/Corrupted Identity. If the secret key of an identity is compromised by an adversary, the identity is a corrupted identity. Else, it is an uncorrupted identity.

Uncorrupted Delegation Chain. Suppose there is a delegation chain under w from ID$_i$ to ID$_j$ (i.e. wjID$_i$! ::: ! ID$_j$). If there is no corrupted identity in the chain, it is an uncorrupted delegation chain. Else, it is corrupted. The delegation chain is built up once either a related re-encryption key is generated or a corresponding re-encryption is constructed.

Definition 2: A unidirectional MH-IBCPRE scheme is IND-sCon-sID-CCA-secure if no PPT adversary A can win the game below with non-negligible advantage. In the game, B is the game challenger and k is the security parameter.

1) Init. A outputs a challenge identity ID 2 f0; 1g and a challenge condition w 2 f0; 1g .
2) Setup. B runs setup(1^k) and returns mpk to A.
3) Phase 1. A is given access to the following oracles.
a) O$_{sk}$(ID): given an identity ID, output sk$_{ID}$ KeyGen(msk; ID).
b) O$_{rk}$(ID$_i$, ID$_i$0, ~~w):~~ on input two distinct iden-tities ID$_i$ and ID$_i$0, and a condition w, output

^{rk}w;ID$_i$!ID$_i$0 ReKeyGen(ID$_i$, sk$_{IDi}$, ID$_i$0, w), where sk_{IDi} KeyGen(msk, ID_i).

c) O_{re}(ID_i, ID_i0, w, $C_{l;IDi;w}$): on input two distinct identities ID_i and ID_i0, a condition w, and an l-level ciphertext $C_{l;IDi;w}$ under ID_i and w, output ^{C}l+1;ID_i;w $^{ReEnc(rk}$w;ID_i!ID_i0 $^{, C}$l;ID_i;w$^{),}$ where ^{rk}w;ID_i!ID_i0 ReKeyGen(ID_i, $^{sk}ID_i$, ID_i0, w), sk_{IDi} KeyGen(msk, ID_i).

$^{d)}$ Odec$^{(ID}$i$^{; C}$l;ID_i;w$^{):}$ on input an identity ID_i, and an l-level ciphertext $C_{l;IDi;w}$, output m $^{Dec(sk}ID_i$ $^{; C}$l;ID_i;w$^{),}$ where $^{sk}ID_i$ KeyGen(msk; ID_i).

In this phase the followings are forbidden to issue:

O_{sk}(ID) for any ID, if there is an uncorrupted delegation chain under w from ID to ID, or ID = ID.

O_{rk}(ID_i; ID_i0; w) for any ID_i; ID_i0, if there is an uncorrupted delegation chain under w from ID
to ID_i or ID = ID_i, but ID_i0 is in a corrupted delegation chain.

4) Challenge. A outputs two equal length messages m_0, m_1, and a set of identities fIDi g$^{j=l\ \ 1}$ to B. B computes
j j=1
$C_{l\ ;ID\ ;w}$ as
ReEnc(ReKeyGen($ID_{il\ 1}$; $sk_{IDil\ 1}$; ID ; w); $^{ReEnc(ReKeyGen(ID}$i$_{l\ 2}$ $^{;}$ $^{sk}ID_{il\ 2}$ $^{; ID}$i$_{l\ 1}$ $^{; w\ );}$
:::; ReEnc(ReKeyGen(ID_{i1} ; sk_{IDi1} ; ID_{i2} ; w); Enc(ID_{i1} ; w ; m_b))));
where l 2; l 2 N; b 2_R f0; 1g. Note that we here put ID to the l level of the ciphertext. This shows no difference from putting it in the first level of the ciphertext since the system supports multi-hop property.

5) Phase 2. Same as in Phase 1 except the followings:

a) O_{re}(ID_i; ID_i0; w ; $C_{l;IDi;w}$): if (ID_i; $C_{l;IDi;w}$) is a derivative of (ID ; $C_{l\ ;ID\ ;w}$), and ID_i0 is in a corrupted delegation chain. As of [11], a derivative of (ID ; $C_{l\ ;ID\ ;w}$) is defined as follows.

i. (ID ; $C_{l\ ;ID\ ;w}$) is a derivative of itself.

ii. If $^{(ID}$i$^{; C}$l;ID_i;w$^{)}$ is a derivative of (ID ; $C_{l\ ;ID\ ;w}$), and $^{(ID}$i$^{0; C}$l^{0};ID_i0;w$^{)}$ is a derivative of $^{(ID}$i$^{; C}$l;ID_i;w$^{),}$ then $^{(ID}$i$^{0; C}$l^{0};ID_i0;w$^{)}$ is a derivative of

(ID ; $C_{l\ ;ID\ ;w}$), where l^0 l l .

iii. If A has issued a re-encryption key query to O_{rk} on (ID_i; ID_i0; w) to obtain the re-encryption $^{key\ rk}$w;ID_i!ID_i0 $^{, and\ achieved}$ ^{C}(l+1;ID_i0;w)

$^{ReEnc(rk}$w;ID_i!ID_i0 $^{; C}$(l;ID_i;w)$^{), then\ (ID}$i^{0,}
^{C}(l+1;ID_i0;w)$^{) is\ a\ derivative\ of\ (ID}i^{; C}$(l;$ID_i$;w) $^{).}$

iv. If A can execute $C_{(l+1;IDi0;w)}$ ReEnc(ReKeyGen(ID_i, sk_{IDi} , ID_i0, w), ^{C}(l;ID_i;w)$^{)\ on\ its\ own,\ then\ (ID}$i^{0,} ^{C}(l+1;$ID_i$0;w)$^{)}$ is a derivative of (ID_i, $C_{(l;IDi;w)}$), where sk_{IDi} KeyGen(msk, ID_i).

v. If A has issued a re-encryption query on $^{(ID}$i$^{; ID}$i$^{0; w; C}$(l;ID_i;w)$^{)}$ and obtained ^{C}(l+1;ID_i0;w)$^{, then\ (ID}$i^{0,} ^{C}(l+1;ID_i0;w)$^{)\ is}$ a derivative of (ID_i, $C_{(l;IDi;w)}$).

b) O_{dec}(ID_i; w ; $C_{l;IDi;w}$): if (ID_i; $C_{l;IDi;w}$) is a derivative of (ID ; $C_{l\ ;ID\ ;w}$). We state that by derivative we mean the issued ciphertext cannot have any delegation link record (including given re-encryption key/re-encrypted ciphertext histories reflected in the delegation chain) related to ID and w .

6) Guess. A outputs a guess b^0 2 f0; 1g. If b^0 = b, A wins. The advantage of A is defined $_1$ as =

$_{Adv}$IND-sCon-sID-CCA$_{(1}$k$_{)\ =}$ P r[b^0 = b] $\bar{2}$.
MH-IBCPRE;A j j

We now proceed to collusion resistance that guarantees that an adversary cannot compromise the entire secret key of a delegator even if it colludes with the delegatee.

3. Conclusions

We introduced a novel notion, anonymous multi-hop identity-based conditional proxy re-encryption, to preserve the anonymity for ciphertext sender/receiver, conditional data sharing and multiple recipient-update. We further proposed a concrete system for the notion. Meanwhile, we proved the system CCA-secure in the standard model under the decisional P -bilinear Diffie-Hellman assumption. To the best of our knowledge, our primitive is the first of its kind in the literature.The document is a template for Microsoft *Word* versions 6.0 or later.

References

[1] G. Ateniese, K. Benson, and S. Hohenberger. Key-private proxy re-encryption. In CT-RSA '09, vol. 5473 of LNCS, pp. 279–294. Springer, 2009.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In NDSS '05, pp. 29–43. Springer, 2005.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM TISSEC, 9(1):1–30, 2006.

[4] M. Bellare and S. Shoup. Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles. In PKC, vol. 4450 of LNCS, pp. 201–216. Springer, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In EUROCRYPT '98, pp. 127–144. Springer, 1998.

[6] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In EUROCRYPT '04, vol. 3027 of LNCS, pp. 223–238. Springer, 2004.

[7] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In EUROCRYPT '05, vol. 3494 of LNCS, pp. 440–456. Springer, 2005.

[8] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In CRYPTO, vol. 4117 of LNCS, pp. 290–307. Springer, 2006.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy. Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In PKC, vol. 5443 of LNCS, pp. 196–214. Springer, 2009.

[10] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In Eurocrypt '04, vol. 3027 of LNCS, pp. 207–222. Springer, 2004.

[11] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In CCS, pp. 185–194. ACM, 2007.

[12] C.-K. Chu and W.-G. Tzeng. Identity-based proxy re-encryption without random oracles. In ISC '07, vol. 4779 of LNCS, pp. 189–202. Springer, 2007.

[13] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput., 33(1):167–226, January 2004.

[14] L. Ducas. Anonymity from asymmetry: new constructions for anonymous HIBE. In CT-RSA ’10, vol. 5985 of LNCS, pp. 148–164. Springer, 2010.

[15] K. Emura, A. Miyaji, and K. Omote. An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system. In EuroPKI ’10, vol. 6711 of LNCS, pp. 77–92. Springer, 2011.

[16] C.-I. Fan, L.-Y. Huang, and P.-H. Ho. Anonymous multireceiver identity-based encryption. Computers, IEEE Transactions on, 59(9):1239–1249, Sept 2010.

[17] M. Green and G. Ateniese. Identity-based proxy re-encryption. In ACNS ’07, vol. 4512 of LNCS, pp. 288–306. Springer, 2007.

[18] A. Ivan and Y. Dodis. Proxy cryptography revisited. In NDSS ’03, 2003.

[19] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, 9(10):1667–1680, 2014.

[20] K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu. An adaptively cca-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. In ISPEC, vol. 8434 of LNCS, pp. 448–461. Springer, 2014.