Journal of Ambient Intelligence and Humanized Computing (2021) 12:2183–2206
https://doi.org/10.1007/s12652-020-02319-x

ORIGINAL RESEARCH

Ternary subset difference revocation in public key framework supporting outsider anonymity

Kamalesh Acharya[1] · **Ratna Dutta**[2]

Received: 15 December 2019 / Accepted: 9 July 2020 / Published online: 7 August 2020

Abstract
Broadcast encryption (BE) is a cryptographic primitive which sends encrypted message to the users securely. The BE scheme proposed by Naor, Naor, and Lotspiech (NNL) in 2001 is a popular BE scheme which uses a binary tree. The advanced access content system standard suggested to use it for digital right management in Blue-ray and DVD-discs. This paper puts forward an efficient broadcast encryption in *public key setting* employing *ternary tree subset difference* method for revocation. Our approach utilizes composite order bilinear group setting to achieve the tree based construction in public key setting. Our second construction is an extension of our first construction and provides *outsider-anonymity* by disabling the revoked users from getting any information of message and *concealing* the set of subscribed users from the revoked users. The construction of Fazio and Perera is the closest one to that of our second scheme (as both of these construction are in public key setting and provides outsider-anonymity). We have reduced the ciphertext size from $r \log N/r$ to $\mathbf{min}\{N/3, N-r, 2r-1\}$. Thus reduces the communication bandwidth. We have also reduced the public key size. Our constructions enjoy the revocation property. Both of our constructions achieve selective semantic security in the standard model under reasonable assumptions and new users can join without updating the pre-existing setup.

Keywords Anonymous broadcast encryption · Outsider-anonymity · Ternary subset difference · Revocation

1 Introduction

Broadcast encryption has received much attention from both the network and cryptography community. It is a cryptographic mechanism that provides the encrypted message to a group of users in such a way that the non-members are unable to get the message. Broadcast encryption was formally introduced by Fiat and Naor (1994), followed by subsequent works in various flavours- revocation scheme (Boneh et al. 2005; Dodis and Fazio 2003; Halevy and Shamir 2002; Lewko et al. 2010), identity based scheme (Delerablée 2007; Li et al. 2018b; Sakai and Furukawa 2007), bilinear map based scheme (Acharya and Dutta 2018a; Acharya 2020; Boneh et al. 2005; Chen et al. 2020; Ge and Wei 2019; Gentry and Waters 2009; Li et al. 2018a; Phan et al. 2013a), multilinear map based scheme (Boneh et al. 2014). Broadcast encryption is widely used in daily life, expanding from pay-TV to digital right management.

The Advanced Access Content System (AACS 2005) is a standard for digital rights management and content protection of the post-DVD generation of optical discs. The AACS standard build upon the basics of the work of Naor et al. (2001b). Since its public release in 2005, it has been adopted for content protection in HD DVD and Blu-ray Disc. Thus tree based broadcast encryption is a popular broadcast encryption mechanism. Followed by Naor et al. (2001b) various tree based schemes developed. Halevy and Shamir (2002) proposed a layered based tree structure. Dodis and Fazio (2003) proposed a generic technique to convert tree based structure (Halevy and Shamir 2002; Naor et al. 2001b) into public key setting. Bhattacherjee and Sarkar (2015) further studied on this. Most of these tree based constructions are in private key setting. In private key broadcast encryption, both the broadcaster and the private key generation center are the same. The broadcaster needs to know the

✉ Kamalesh Acharya
kamaleshiitkgp@gmail.com

Ratna Dutta
ratna@maths.iitkgp.ernet.in

[1] School of Computer Sciences, NISER Bhubaneswar, HBNI, Khurda 752050, India

[2] Department of Mathematics, IIT Kharagpur, Kharagpur 721302, India

secret information for encryption. Therefore the same setup cannot be applicable in two different private key broadcast encryption systems. In public key setting, the broadcaster and the private key generation center are different and the broadcaster encrypts the message without using any secret information. Thus the public key setup is more flexible to use.

Basic security property of public key encryption is data secrecy, whereby no information about the original message gets leaked. It can reveal the set of recipients who will receive the message. In modern world of digital technology, hiding the recipient set from the non-recipient users is of crucial importance. For instance, in satellite TV subscription service, a customer usually expects his identity should not get revealed when ordering a sensitive TV channel. It is required that the subscribed user's identity should remain secret from the other subscribers and outsiders. Barth et al. (2006) introduced an *anonymous broadcast encryption* scheme to address the privacy issue in broadcast encryption.

Outsider anonymous broadcast encryption is another exciting variant of broadcast encryption that achieves security and privacy of the receivers. Consider following *application*: Suppose a group of scientists is working on a secret project. They need to share the documents among themselves. However, the documents and the identities of the involved scientists should be kept secret from the outsiders.

In this type of applications, subscribed user's identity should be kept secret from the outsiders although it need not be concealed from the other subscribers. This notion of anonymity is termed as *outsider-anonymity* by Fazio and Perera (2012). Most of the broadcast encryption schemes do not support privacy property and decryption algorithms in these schemes take the recipient set S or the non-recipient set $\mathbb{R}$ as input (see Fig. 1).

Our contribution Our goal is to devise new tree-based public key broadcast encryption which supports revocation as well as outsider-anonymity. We summarize below the main findings of this work:

(i) Our public key broadcast encryption (PKBE) employs ternary tree subset difference method of Fukushima et al. (2009) to partition subscribed users into groups. For each group, broadcaster generates ciphertext using anonymous hierarchical identity based encryption of Seo et al. (2009). The most related work to our tree based construction OAnoBE, which supports outsider-anonymity in public key setting is the scheme of Fazio and Perera (2012). We have compared the efficiency in ciphertext size with Fazio and Perera (2012) in Fig. 2. Integrating the *ternary SD revocation method*, we reduce the size of partition, and consequently the ciphertext size, leading to a significant improvement over (Fazio and Perera 2012). A comparative summary of tree based broadcast encryption schemes are outlined in Table 1.

(ii) Construction of Seo et al. (2009) sends one message to one user. Thus sending message to a group of users needs huge computation cost and communication bandwidth. We have used the construction of Seo et al. (2009) to generate a broadcast encryption scheme. Thus one encryption can send different messages to different group of users. Thus both of our constructions are different from Seo et al. (2009).

(iii) Broadcast encryption can be broadly classified into two: public key BE and private key BE. In private key BE, the broadcaster plays the role of the private key generation center and consequently, knows sensitive information such as master secret key whose disclosure may compromise the security. The same setup cannot be used by different broadcasters in private key setting. The encrypter either stores the secret keys or computes them during the encryption. On the other hand, public key BE considers the private key generation center and the broadcaster as different entities and performs encryption with the help of public parameters. It reduces the workload of the broadcaster by employing a private key gen-

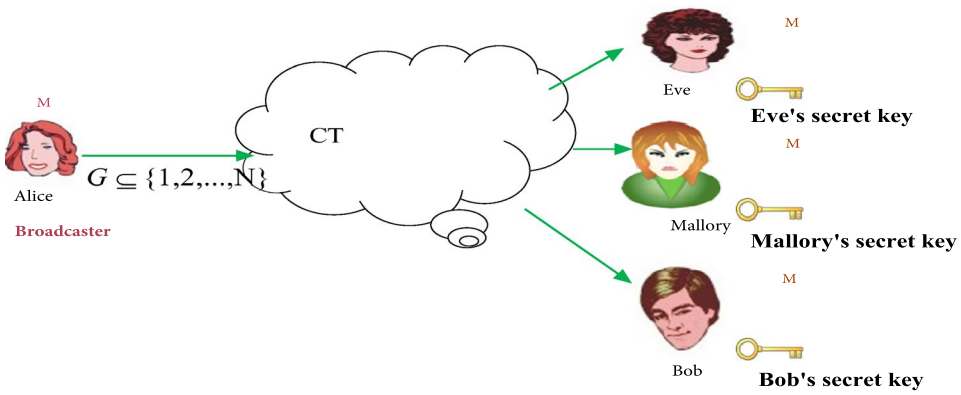

Fig. 1 Broadcast encryption

Table 1 Comparison of various tree based broadcast encryption schemes

Scheme	PK size	SK size	CT size	Anon	SM	MC	RO	Public
Naor et al. (2001b)	–	$O(\log_2 N.\kappa)$	$O(r \log_2 \frac{N}{r}.\kappa_T)$	No	Selective	IND-CPA	No	No
	–	$O(\log_2^2 N.\kappa)$	$O(r.\kappa_T)$	No	Selective	IND-CPA	No	No
Halevy and Shamir (2002)	–	$O(\log_2^{1+\epsilon} N.\kappa)$	$O(\frac{r}{\epsilon}.\kappa_T)$	No	Selective	IND-CPA	No	No
Fukushima et al. (2009)	–	$O(log_3^2 N.\kappa)$	$O(r.\kappa_T)$	No	Selective	IND-CPA	No	No
Bhattacherjee and Sarkar (2015)	–	$((\chi_k - 1)l_0(l_0+1)/2).\kappa$	$\min\{\frac{N}{k}, N-r, 2r-1\}.\kappa_T$	No	–	–	–	No
Dodis and Fazio (2003)	$O(N.\kappa)$	$O(\log_2 N.\kappa)$	$O(r \log_2 \frac{N}{r}.\kappa_T)$	No	–	–	–	Yes
	$O(N.\kappa)$	$O(log_2^2 N.\kappa)$	$O(r.\kappa_T)$	No	–	–	–	Yes
Fazio and Perera (2012)	$(N+2).\kappa$	$(\log_2 N+1).\kappa$	$(r \log_2 \frac{N}{r}).\kappa_T$	Outsider	Adaptive	IND-CCA	No	Yes
PKBE	$(\log_3 N+6).\widetilde{\kappa}$	$O(\log_3{}^2 N.\widetilde{\kappa})$	$\leq \min\{\frac{N}{3}, N-r, 2r-1\} \cdot \tilde{\kappa}_T$	No	Selective	IND-CPA	No	Yes
OAnoBE	$(\log_3 N+6).\widetilde{\kappa}$	$O(\log_3{}^2 N.\widetilde{\kappa})$	$\min\{\frac{N}{3}, N-r, 2r-1\}.\widetilde{\kappa}_T$	Outsider	Selective	IND-CPA	No	Yes

PK public key, *SK* secret key, *CT* ciphertext, *Anon* anonymity, '*No-of- dec*' Number of decryption, *SM* security model, *MC* message confidentiality, *RO* random oracle, *IND-CP(C)A* indistinguishability of ciphertext under chosen plaintext (ciphertext) attack. Here, N is total number of users and r is the number of revoked users and l is ciphertext length. χ_k=no. of cyclotonic cosets of k bit string, $l_0 = \log_k n$, $\epsilon > 0$, κ= bit size of an element of prime order source group, κ_T =bit size of an element of prime order target group, $\widetilde{\kappa}$= bit size of an element of composite order source group, $\widetilde{\kappa}_T$ = bit size of an element of composite order target group.

Scheme (Bhattacherjee and Sarkar 2015; Fukushima et al. 2009; Halevy and Shamir 2002; Naor et al. 2001b) are in private key broadcast encryption scheme and Bhattacherjee and Sarkar (2015), Dodis and Fazio (2003) are generic construction

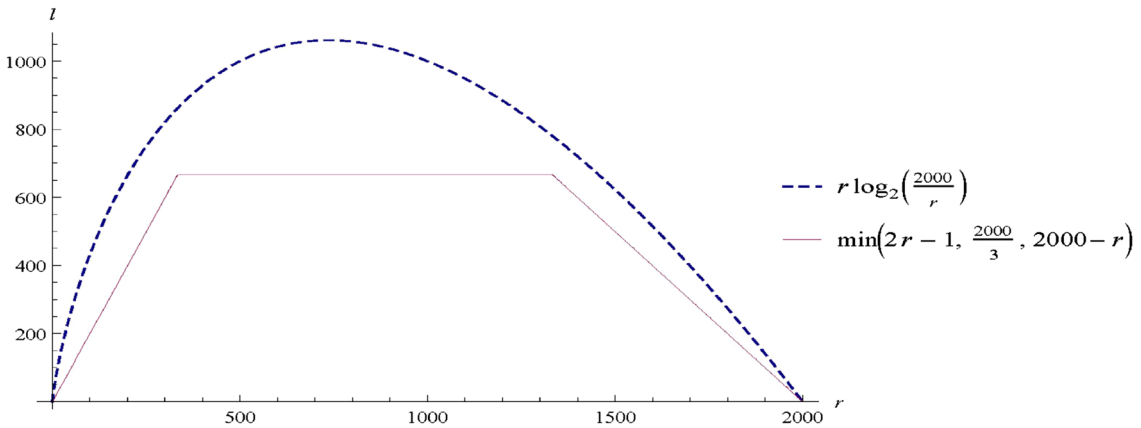

Fig. 2 Comparison of cover size (l) against revoked user (r) [number of users N =2000]

eration center, which is required in many broadcast mechanism. Existing tree based broadcast encryption (Bhattacherjee and Sarkar 2015; Halevy and Shamir 2002; Naor et al. 2001b) are in private key setting where the broadcaster and the private key generation center are same. The public key broadcast encryption of Dodis and Fazio (2003) is in generic model. Both of our tree based constructions are in public key setting.

(iv) Achieving anonymity is another task in the modern era of digital technology. Most of the tree based constructions do not achieve it. Our second construction OAnoBE achieves outsider-anonymity by disabling the outsiders to know about the recipient set. Outsider-anonymity is weaker than full anonymity in the sense that the user identities are not secret to any user of the group. But there are some applications where it is required to share the message among the subscribers (as discussed in page 2) and thus practical to use.

(v) More interestingly, our scheme enjoys the revocation property which is one of the most significant requirement in the broadcast encryption setting. To facilitate revocation, subscribed user uses the set of secret keys in such a way that he will capable to recover the message. None of the existing anonymous constructions discusses the revocation process.

(vi) Furthermore, new users can join any time without updating the pre-existing public key and secret key, provided the number of subscribed users in the system does not exceed the maximum number of users allowed in the system.

Discussion on Tree-based Schemes of Table 1 Naor et al. (2001b) proposed two construction using binary complete subtree and subset difference method respectively. Halevy and Shamir (2002) proposed a scheme using layered subset difference method. Bhattacherjee and Sarkar (2015) proposed a scheme using k-ary tree. Fukushima et al. (2009) proposed a scheme using Ternary subset difference method. All of these schemes are private key broadcast encryption scheme. Thus, these schemes send message to group of users. But, these schemes do not provide any kind of anonymity and not in public key setting. Now we will discuss some public key tree based broadcast encryption schemes. In public key setting, we can use the same Setup for different broadcast encryption schemes as the broadcaster does not need any secure information for encryption. Dodis and Fazio (2003) proposed a public key variant of Naor et al. (2001b). Fazio and Perera (2012) proposed outsider-anonymous broadcast encryption in public key setting. We have provided two constructions. First one reduces ciphertext size compare to the scheme of Fazio and Perera (2012). The second one provides outsider-anonymity by hiding the set of subscribed users from revoked users and also reduces ciphertext size.

Organization The rest of the paper is organized as follows. We discuss related works in Sect. 2. Section 3 provides necessary definitions and background materials. We describe our main constructions in Sect. 4. Section 5 gives the implementation results. We finally conclude in Sect. 6.

2 Related works

Cryptography is a way of sending the message (data) securely to a receiver in such a way that a third party cannot understand the message. In general, cryptographic encryption schemes (e.g., ElGamal 1985; Hu et al. 2016; Liu and Ke 2019; Xu et al. 2020) are one to one where a message is communicated between a sender and a receiver. The broadcast encryption protocols helps to send a message to a group of users. The concept of broadcast encryption was proposed by Fiat and Naor (1994), following which a wide variety of schemes have been proposed. In this section, we discuss various type of broadcast encryption schemes such as revocation based construction, algebraic construction using bilinear and multilinear map, identity based construction, anonymous construction, and others. Depending on size of subscribed and revoked users, BE can be divided into- Subscription based broadcast encryption (e.g., Boneh et al. 2005, 2014; Gentry and Waters 2009; Phan et al. 2013a) and revocation based broadcast encryption (e.g., Delerablée et al. 2007; Dodis and Fazio 2003; Halevy and Shamir 2002; Lewko et al. 2010; Naor et al. 2001b). Revocation based broadcast encryption schemes are useful where $r \ll N$ as smaller revocation set reduces the computation overhead. Here r is the number of revoked users and N is the total number of users supported by the system. Subscription based broadcast encryption schemes are useful where $N - r \ll N$ i.e., subscriber's set is smaller.

2.1 BE depending on applications

Depending on application BE can be classified into following like- Identity based BE, Traitor Tracing, Distributed BE, Hierarchical BE, Broadcast Encryption with dealership, Recipient Revocable BE, Anonymous BE, Broadcast encryption with personalised messages, Multi-channel BE etc.

1. *Identity Based Scheme* Identity based encryption scheme was introduced by Shamir (1985). Delerablée (2007) proposed first identity based broadcast encryption scheme in Asiacrypt 2007. The scheme is secure under chosen plaintext attack in selective ID model under the GDDHE assumption. Sakai and Furukawa (2007) came up with an identity based broadcast encryption scheme on additive bilinear group with constant private key and ciphertext size. In Asiacrypt 2008, Boneh and Hamburg (2008) proposed generalised identity based encryption scheme. The scheme is key indistinguishable under adaptive key exchange attack in generic bilinear group model with random oracle.
2. *Traitor Tracing Scheme* An important property on broadcast encryption scheme is the traceability. Traitor tracing scheme was introduced by Chen et al. (1994) on Crypto 1994. Boneh et al. (2006) proposed first collision resistance scheme using private linear broadcast encryption. The scheme is secure under the bilinear subgroup decision and subgroup decision assumption. Trace and revoke scheme is a combination of broadcast encryption and tracing scheme. Boneh and Waters (2006) proposed a scheme which is secure under decisional three party Diffie–Hellman assumption. Boneh and Zhandry (2014) proposed a scheme using indistinguishability obfuscation. Security of this scheme lies on security of underlying pseudo random function.
3. *Distributed Broadcast Encryption Scheme* In ProvSec 2014, Wu et al. (2011) proposed another variant of broadcast encryption called as distributed broadcast encryption system in which instead of key generation centre, users creates secret key for themselves. Boneh and Zhandry (2014) proposed several schemes using

indistinguishability obfuscation in Crypto 2014. One of them is distributed broadcast encryption and achieves IND-CCA security under the existence of multiparty key exchange protocol.

4. *Hierarchical Broadcast Encryption Scheme* In ACISP 2014, Liu et al. (2014) proposed a new primitive called as hierarchical identity based broadcast encryption scheme where user can delegate their decryption capability to their descendent users. They proposed a CCA secure version Liu et al. (2015) in IJIS 2015.
5. *Broadcast Encryption with Dealership Scheme* Gritti et al. (2015) proposed broadcast encryption with dealership scheme in which instead of broadcaster, a dealer selects a set of subscribed users. The scheme is semi-static IND-CPA secure under N-DBDHE assumption. In this construction broadcaster need to rely on user response to detect a dishonest dealer. Acharya and Dutta (2016) has solved the problem and proposed a scheme with constant communication.
6. *Recipient Revocable Broadcast Encryption* Susilo et al. (2016) introduced recipient revocable broadcast encryption (RRBE) in AsiaCCS 2016. The scheme provides selective security under the $(\hat{f}, \phi, F)$-General Decisional Diffie–Hellman Exponent ($(\hat{f}, \phi, F)$-GDDHE) assumption. The security proof uses random oracles. Lai et al. (2016) proposed an adaptively secure scheme with constant storage. The scheme achieves adaptive security under the Bilinear Diffie–Hellman Exponent problem in the random oracle model. Recently, Lai et al. (2017) proposed another scheme which has similar security property. Schemes Lai et al. (2016), Lai et al. (2017) achieve anonymity property which provides user privacy. Acharya and Dutta (2018b) proposed two constructions in standard model with comparable parameter sizes.
7. *Anonymous Scheme* In FCDS 2006, Barth et al. (2006) proposed a new variant of broadcast encryption, called as *private broadcast encryption* or *anonymous broadcast encryption* (AnoBE). The scheme is selective IND-CCA secure in the random oracle model. An adaptive IND-CCA secure scheme with the same parameters and standard security model was developed by Libert et al. (2012) in PKC 2012. In IJNS 2014, Ren et al. (2014) came up with the first identity based *anonymous broadcast encryption* scheme. The scheme is adaptive IND-CPA secure under asymmetric decisional Bilinear Diffie–Hellman assumption. Fazio and Perera (2012) proposed an anonymous scheme with sublinear ciphertext size in PKC 2012. It achieves outsider-anonymity where no revoked user achieve any information about the subscribed users. Both the schemes (Barth et al. 2006; Libert et al. 2012) are generic. Recipient Revocable Broadcast Encryption Scheme (Lai et al. 2016, 2017 also achieves anonymity (we have discussed in the previous paragraph).
8. *Broadcast Encryption with Personalized Messages* Ohtake et al. (2010) proposed the first broadcast encryption with personalized messages (BEPM) scheme. Security is proven in the selective semantic security model under the Decisional Bilinear Diffie-Hellman Exponent (DBDHE) assumption. Xu et al. (2015) attempted to reduce the public parameter size using multilinear maps (Boneh and Silverberg 2003; Coron et al. 2013; Garg et al. 2013a, b) which is unfortunately flawed. Acharya and Dutta (2017) proposed three constructions. Their first construction achieves similiar security property but second one archives adaptive security. Third construction reduces public parameter size using the multilinear map and achieves selective semantic security under Decisional Hybrid Diffie–Hellman Exponent (DHDHE) assumption.
9. *Multi-Channel Broadcast Encryption* Phan et al. (2013b) developed first multi-channel broadcast encryption (MCBE) scheme in private key setting. The scheme achieves selective indistinguishability against chosen plaintext attack under the decisional bilinear Diffie–Hellman exponent (DBDHE) assumption. Later, Zhao and Li (2013) improved this work and provided an MCBE scheme with short public parameter by reducing the number of exponentiations in the public parameters of the MCBE of Phan et al. (2013b). It gives similar security.

2.2 BE depending on key generation process

Depending upon key generation process, BE can be divided into public key and private key setting.

1. *Private key BE* Private key BE uses same key for encryption and decryption. In private key setting, both the private key generation center and broadcaster are the same. In Crypto 2001, Naor et al. (2001b) suggested two private key broadcast encryption schemes. These schemes are indistinguishable under chosen ciphertext attack (IND-CCA) on "key indistinguishability" assumption. A layer-based subset difference scheme was proposed by Halevy and Shamir (2002) in Crypto 2002. It achieves similar security. Ke et al. (2015) proposed constructions based on balanced incomplete block design and strong partially balanced incomplete block design. Moreover, it enhances the security level.
2. *Public key BE* Private key BE uses same keys for encryption and decryption. More specifically, broadcaster needs some secure information for encryption. Hence, the same Setup cannot be used in different private key BE constructions. Public key BE solves the

issue and uses different keys for encryption and decryption purpose. There are various public key constructions like- Acharya and Dutta (2016), Boneh and Zhandry (2014), Boneh et al. (2005), Delerablée (2007), Lewko et al. (2010). We have discussed these in subsection 2.1.

3 Preliminaries

Notation Throughout the paper, we will follow notations and abbreviations of Table 2.

3.1 Public key broadcast encryption

A *public key broadcast encryption* scheme PKBE= (Setup, KeyGeneration, Encrypt, Decrypt) consists of 3 probabilistic polynomial time (PPT) algorithms Setup, KeyGeneration, Encrypt and 1 deterministic polynomial time algorithm Decrypt.

Setup(N, λ): The private key generation centre (PKGC) takes the total number of users N and security parameter λ and constructs a public key PK and a master key MK.

KeyGeneration(PK, MK, i): Receiving the public key PK, master key MK and a subscribed user i, the PKGC outputs secret key sk_i of user i.

Encrypt($\mathbb{R}$, PK, m): The broadcaster takes the set of revoked users $\mathbb{R}$, the public key PK and a message m as input and outputs a ciphertext C.

Table 2 Notations and abbreviations

$\perp$	Null string
$y \in_R S$	Variable y is taken from set S Following an uniform distribution
$\|X\|$	Cardinality of the set X
$[m]$	$\{1, \ldots, m\}$.
$A \cap B$	Intersection of set A, B
PN(v)	Path node of v
HN(v)	Hanging node of v
PPT	Probabilistic polynomial time
PK	Public key
SK	Secret key
CT	Ciphertext

Decrypt(PK, sk_i, $\mathbb{R}$, C): On input secret key sk_i, set of revoked users $\mathbb{R}$, ciphertext C encrypting message m and public key PK, a subscribed user i outputs message m.

Correctness The correctness of the scheme lies in the fact that m can be retrieved from C if the user is outside of the revoked set $\mathbb{R}$, i.e.,

$$\text{Decrypt}(\text{PK}, \text{KeyGeneration}(\text{PK}, \text{MK}, i), \mathbb{R}, \text{Encrypt}(\mathbb{R}, \text{PK}, m)) = m,$$

for every revoked set $\mathbb{R}$, every message m.

Security game We define below *selective semantic security* of PKBE= (Setup, KeyGeneration, Encrypt, Decrypt) following Gentry and Waters (2009) in the form of an indistinguishability game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Initialization The adversary $\mathcal{A}$ gives revoked set (i.e., the set of non-subscribed users) $\mathbb{R}$ to the challenger $\mathcal{C}$.

Setup The challenger $\mathcal{C}$ runs (PK, MK) $\leftarrow$ Setup(N, λ). It keeps MK secret to itself and makes PK public.

Phase 1 The adversary $\mathcal{A}$ sends key generation query for $i_1, \ldots, i_m \in \mathbb{R}$ to $\mathcal{C}$ and receives the secret key $sk_i \leftarrow$ KeyGeneration(PK, MK, i).

Challenge The adversary $\mathcal{A}$ sends two equal length messages m_0, m_1 to $\mathcal{C}$. The challenger $\mathcal{C}$ chooses a random $b \in \{0, 1\}$, makes $C_b \leftarrow$ Encrypt($\mathbb{R}$, PK, m_b) and sends C_b as challenge ciphertext to $\mathcal{A}$.

Phase 2 This is similar to Phase 1 key generation query. The adversary $\mathcal{A}$ sends key generation query for $i_{m+1}, \ldots, i_q \in \mathbb{R}$ to $\mathcal{C}$ and receives secret key $sk_i \leftarrow$ KeyGeneration(PK, MK, i).

Guess The adversary $\mathcal{A}$ output a guess $b' \in \{0, 1\}$ of b.

The adversary $\mathcal{A}$ wins the game if $b'= b$ and its advantage is defined as $Adv_{\mathcal{A}}^{\text{PKBE-IND-CPA}} = |Pr(b' = b) - \frac{1}{2}|$. The probability is over random bits used by $\mathcal{C}$ and $\mathcal{A}$.

Definition 1 Broadcast encryption scheme PKBE is (t, q, ϵ) -IND-CPA secure if $Adv_{\mathcal{A}}^{\text{PKBE-IND-CPA}} \leq \epsilon$ for every adversary $\mathcal{A}$ running for at most t time and making at most q key generation queries.

As our public key broadcast encryption supports outsider-anonymity, we will explain outsider anonymous public key broadcast encryption and its security proof.

• *Outsider-anonymous broadcast encryption*

In contrast to usual broadcast encryption, the decryption algorithm in OAnoBE does not require the set of subscribers or the set of revoked users as input. Other algorithms are identical to public key broadcast encryption.

Security game

We define below *selective semantic security* of OAnoBE= (Setup, KeyGeneration, Encrypt, Decrypt) following outsider anonymous scheme of Fazio and Perera (2012) and revocation scheme of Naor et al. (2001b) in the form of an indistinguishability game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Initialization	The adversary $\mathcal{A}$ gives two revoked sets (i.e., the set of non-subscribed users) $\mathbb{R}_0, \mathbb{R}_1$ to the challenger $\mathcal{C}$, where $\mathbb{R}_0, \mathbb{R}_1$ contain equal number of revoked users.
Setup	This is similar to PKBE.
Phase 1	The adversary $\mathcal{A}$ sends key generation query for $i_1, \ldots, i_m \in \mathbb{R}_0 \cap \mathbb{R}_1$ to $\mathcal{C}$ and receives the secret key $sk_i \leftarrow \mathsf{KeyGeneration}(\mathsf{PK}, \mathsf{MK}, i)$.
Challenge	The adversary $\mathcal{A}$ sends two equal length messages m_0, m_1 to $\mathcal{C}$. The challenger $\mathcal{C}$ chooses a random $b \in \{0,1\}$, makes $C_b \leftarrow \mathsf{Encrypt}(\mathbb{R}_b, PK, m_b)$ and sends C_b as challenge ciphertext to $\mathcal{A}$.
Phase 2	This is similar to Phase 1 key generation query. The adversary $\mathcal{A}$ sends key generation query for $i_{m+1}, \ldots, i_q \in \mathbb{R}_0 \cap \mathbb{R}_1$ to $\mathcal{C}$ and receives secret key $sk_i \leftarrow \mathsf{KeyGeneration}(\mathsf{PK}, \mathsf{MK}, i)$.
Guess	The adversary $\mathcal{A}$ output a guess $b' \in \{0,1\}$ of b.

The adversary $\mathcal{A}$ wins the game if $b'=b$ and its advantage is defined as $Adv_{\mathcal{A}}^{\mathsf{OAnoBE-IND-CPA}} = |Pr(b' = b) - \frac{1}{2}|$. The probability is over random bits used by $\mathcal{C}$ and $\mathcal{A}$.

Definition 2 Broadcast encryption scheme OAnoBE is (t, q, ϵ) -IND-CPA secure if $Adv_{\mathcal{A}}^{OAnoBE-IND-CPA} \leq \epsilon$ for every adversary $\mathcal{A}$ running for at most t time and making at most q key generation queries.

3.2 Complexity assumptions

Definition 3 Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative groups of order $n = pq$, where bit length of n is $|n| = \lambda$ and p, q are prime. Let g be a generator of $\mathbb{G}$. A bilinear map $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$ is a function having the following properties:

1. $e(u^a, v^b) = e(u, v)^{ab}$, $\forall\, u, v \in \mathbb{G}$ and $\forall\, a, b \in \mathbb{Z}$.
2. The map is non degenerate, i.e., $e(g, g)$ is generator of $\mathbb{G}_T$.

The tuple $\mathbb{S} = (n, \mathbb{G}, \mathbb{G}_T, e)$ is said to be a composite order bilinear group system.

Let $\mathbb{G}_p, \mathbb{G}_q$ stand for subgroups of $\mathbb{G}$ of order p, q respectively, $\mathbb{G}_{T,p}, \mathbb{G}_{T,q}$ denote subgroups of $\mathbb{G}_{\mathbb{T}}$ of order p, q respectively and g_p, g_q are generators of $\mathbb{G}_p$ and $\mathbb{G}_q$ respectively. We use the notation $x \in_R S$ to denote x is a random element of S. Let N,R be sets of natural and real numbers respectively. The function $\epsilon(\lambda)$ is said to be a *negligible function* if for every positive integer c, $\exists$ an integer N_c such that for every $\lambda > N_c$, $\epsilon(\lambda) \leq \frac{1}{\lambda^c}$.Let $\epsilon : \mathrm{N} \rightarrow \mathrm{R}$ be a function. If $\exists\, d \in \mathrm{N}$ such that $\epsilon(\lambda) \leq \frac{1}{\lambda^d}$ then ϵ is *negligible function.*

– *l-Weak decisional bilinear Deffie–Hellman inversion(l-wDBDHI*) Assumption* (Seo et al. 2009):
  input: $Z = (\mathbb{S}, h, g_q, g_p, g_p^{\alpha}, \ldots, g_p^{\alpha^l}), T$, where $h \in_R \mathbb{G}_p, \alpha \in_R \mathbb{Z}_n, T \in_R \mathbb{G}_{T,p}$.
  output: Yes if $T = e(g_p, h)^{\alpha^{l+1}}$; No otherwise.
  The advantage of adversary $\mathcal{A}$ in solving the above problem is $Adv_{\mathcal{A}}^{l-wDBDHI^*} = |Pr[\mathcal{A}(Z, e(g_p, h)^{\alpha^{l+1}}) = 1] - Pr[\mathcal{A}(Z, T) = 1]|$.
  l-wDBDHI Assumption:* For any PPT algorithm $\mathcal{A}$ above advantage is negligible, i.e., $Adv_{\mathcal{A}}^{l-wDBDHI^*} \leq \epsilon(\lambda)$, where $\epsilon(\lambda)$ is a negligible function in security parameter λ.
– *l-Composite decisional Deffie Hellman (l-cDDH) Assumption* (Seo et al. 2009):
  input $Z = (\mathbb{S}, h, g_q, g_p, g_p^{\alpha}, \ldots, g_p^{\alpha^{l+1}}.R_1, (g_p^{\alpha^{l+1}})^{\beta}.R_2), T$, where $R_1, R_2 \in_R \mathbb{G}_q, \alpha, \beta \in_R \mathbb{Z}_n, T \in_R \mathbb{G}$.
  output: Yes if $T = g_p^{\beta}.R_3$, for some $R_3 \in_R \mathbb{G}_q$; No otherwise. The advantage of $\mathcal{A}$ in solving the above problem is $Adv_{\mathcal{A}}^{l-cDDH} = |Pr[\mathcal{A}(Z, g_p^{\beta}.R_3) = 1] - Pr[\mathcal{A}(Z, T) = 1]|$
  l-cDDH Assumption: For any PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{l-cDDH}$ is negligible.
– *Bilinear Subset Decision (BSD) Assumption* Seo et al. 2009:
  input: $Z = (\mathbb{S}, g_q, g_p), T$, where $T \in_R \mathbb{G}_T$.
  output: Yes if $T \in \mathbb{G}_{T,p}$; No otherwise. The advantage of adversary $\mathcal{A}$ in solving the above problem is $Adv_{\mathcal{A}}^{BSD} = |Pr[\mathcal{A}(Z, T) = 1] - Pr[\mathcal{A}(Z, T^*) = 1]|$, where $T \in \mathbb{G}_{T,p}$, $T^* \in_R \mathbb{G}_T$.
  BSD Assumption: For any PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{BSD}$ is negligible.

3.3 Ternary subset difference framework

Our scheme is based on ternary tree SD method as introduced in Fukushima et al. (2009). Consider a complete ternary tree T in which the users lie at the leaf nodes. This system can accommodate at most N users, where N is a

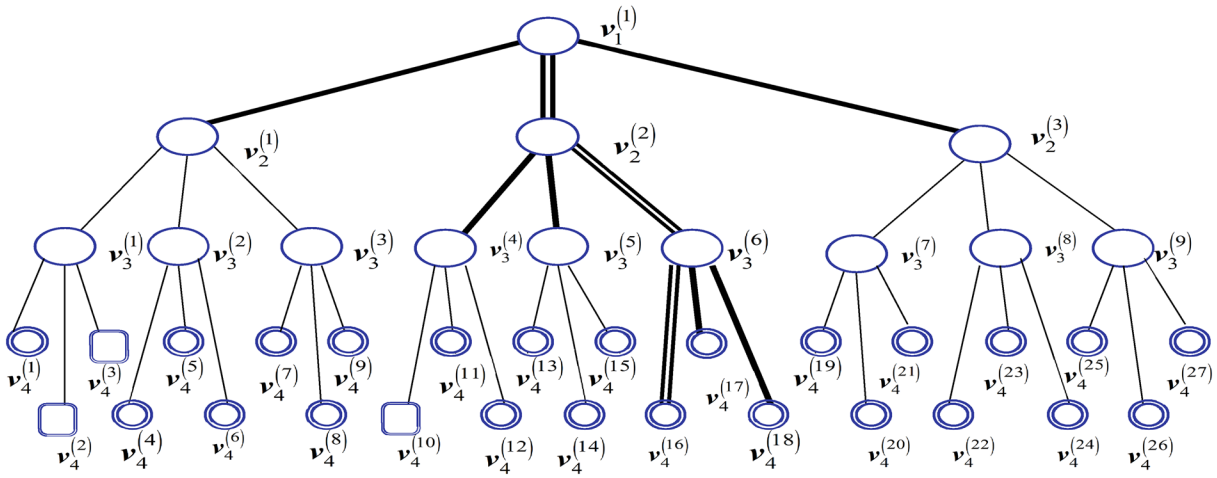

Fig. 3 Labeling of nodes of a complete ternary tree with revoked users $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$, where double-thick lines represent a path from the root node $v_1^{(1)}$ to the user u at $v_4^{(16)}$, thick lines denote the edges just hanging off this path, circular nodes represent the internal nodes, rectangular nodes are the revoked users and double circular nodes stand for the subscribed users

power of 3. We level the nodes as in Fig. 3. The root node $v_1^{(1)}$ of T is at level 1. The left, middle, right child of $v_i^{(l_i)}$ are $v_{i+1}^{(l_{i+1})}$, $l_{i+1} = 3l_i - 2, 3l_i - 1, 3l_i$ respectively. We denote by $T_{v_i^{(l_i)}}$, the complete subtree rooted at $v_i^{(l_i)}$. For a set of revoked users R, ST(R) denotes the Steiner tree, i.e., the minimal subtree of $T(= T_{v_1^{(1)}})$ connecting all the members of the set of revoked users R with the root. For a node $v_i^{(l_i)}$, its parent node is defined as

$$\mathsf{parent}(v_i^{(l_i)}) = \begin{cases} v_{i-1}^{\left(\left\lceil \frac{l_i}{3} \right\rceil\right)} & \text{if it is a left or a middle child} \\ v_{i-1}^{\left(\frac{l_i}{3}\right)} & \text{if it is a right child} \end{cases}$$

Path connecting the root to the user u at a leaf node $v_L^{(l_L)}$ is denoted by $\mathsf{path}(v_L^{(l_L)})$. The nodes on $\mathsf{path}(v_L^{(l_L)})$ are referred as $\mathsf{PN}(v_L^{(l_L)})$ and the nodes just hanging of the nodes in $\mathsf{PN}(v_L^{(l_L)})$ are defined as $\mathsf{HN}(v_L^{(l_L)})$.

Definition 4 A *chain* is a sequence of nodes $v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_j)}$ or $v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$ ($v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$ are siblings) having the following properties in ST(R):

(i) $v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_{j-2}^{(l_{j-2})}$ have one child each.
(ii) $v_{j-1}^{(l_{j-1})}$ is either a node with one child or two children.
(iii) Each of $v_j^{(l_{j_1})}, v_j^{(l_{j_2})}$ is either a node with three children or leaf node.
(iv) $v_i^{(l_i)}$ is the root node or $\mathsf{parent}(v_i^{(l_i)})$ is a node with two or three children.

We use the notation $S_{v_i^{(l_i)}, v_j^{(l_j)}}$ to represent the set of users in $T_{v_i^{(l_i)}}$ minus that in $T_{v_j^{(l_j)}}$ and $S_{v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}}$ to represent the set of users in $T_{v_i^{(l_i)}}$ minus that in $T_{v_j^{(l_{j_1})}}$ and $T_{v_j^{(l_{j_2})}}$. We say that $S_{v_i^{(l_i)}, v_i^{(l_j)}}$ is the subset cover generated by the chain $v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_j)}$ and $S_{v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}}$ is the subset cover generated by the chain $v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_{j_1)}}; v_j^{(l_{j_2})}$, where $v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$ are siblings.

We assign node *identity* $I_i^{(l_i)} \in \mathbb{Z}_n$ to each level i node $v_i^{(l_i)}$, where $1 \le i \le \log_3 N + 1, 1 \le l_i \le 3^{i-1}$. At level i, the *hierarchial identity* of a node $v_i^{(l_i)}$ is $\mathsf{ID}|_{v_i^{(l_i)}} = (I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_i^{(l_i)}) \in (\mathbb{Z}_n)^i$, where $I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_i^{(l_i)}$ are the identities of nodes in the path from the root $v_1^{(1)}$ to node $v_i^{(l_i)}$. All the nodes in the same level are assigned different hierarchial identities.

Definition 5 Let the node $v_j^{(l_j)}$ be in the subtree $T_{v_i^{(l_i)}}$ rooted at $v_i^{(l_i)}$ and the hierarchial identity of the node $v_j^{(l_j)}$ be $(I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_j^{(l_j)})$. The modified hierarchial identity of a node $v_j^{(l_j)}$ in $T_{v_i^{(l_i)}}$ is defined to be $(I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)})$, i.e., the hierarchial identity from i-th position to rest in $\mathsf{ID}|_{v_j^{(l_j)}}$.

Algorithm 1 FindChain

input: A revoked user.
output: Chain generating the subset cover $S_{v_i^{(l_i)},J}$ of the subscribed users.

1. Follow the path from the revoked user to the root.
2. ***if*** a node is found on the path with less than 3 children ***then***
   (a) ***if*** $\exists$ only one child $v_j^{(l_{j_1})}$ ***then*** set $J = v_j^{(l_{j_1})}$.
   (b) ***if*** $\exists$ two children $v_j^{(l_{j_1})}$, $v_j^{(l_{j_2})}$ ***then*** set $J = v_j^{(l_{j_1})} + v_j^{(l_{j_2})}$.
   (c) from $v_j^{(l_{j_1})}$, proceed until a node $v_i^{(l_i)}$ is found on the path whose parent has two or three children or it is the root node.
   (d) ***return*** sequence of nodes $v_i^{(l_i)}$ to $v_j^{(l_{j_1})}$ or $v_i^{(l_i)}$ to $v_j^{(l_{j_1})}$; $v_j^{(l_{j_2})}$ on the path as the chain generating the subset cover $S_{v_i^{(l_i)},J}$ of the subscribed users.
3. ***end if***

Cover finding Algorithm Cover finding Algorithm FindCover invokes procedure FindChain to generate chain corresponding to a given set R of revoked users and partitions the subscribed users into collection of disjoint subset covers. Different subset covers are generated from different chains. Algorithm 2 formally describes FindCover.

Algorithm 2 FindCover

input: Set of revoked users R.
output: Cover obtained by ternary SD method.

1. Set Cover $= \phi$.
2. Invoke FindChain for each revoked user in R and generate all the chains.
3. ***for*** each chain in the steiner tree ST(R) of R ***do***
   (a) Let a chain contains nodes $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$, $\ldots$, $v_j^{(l_j)}$ or $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$, $\ldots$, $v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$.
   (b) Add $S_{v_i^{(l_i)},J}$ ($J = v_j^{(l_j)}$ or $v_j^{(l_{j_1})} + v_j^{(l_{j_2})}$) to the Cover and add $v_i^{(l_i)}$ to R and remove $v_j^{(l_j)}$ or $v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$ from R.
4. ***end for***
5. Take the new revoked set R and goto step 2.

Lemma 1 *The cover size for ternary SD is at most* $\min\{\frac{N}{3}, N-r, 2r-1\}$, *where N is maximum number of users, r is number of revoked users.*

Proof For each chain $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$, $\ldots$, $v_j^{(l_j)}$ or $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$,$\ldots$, $v_j^{(l_{j_1})}; v_j^{(l_{j_2})}$, parent($v_i^{(l_i)}$) is either the root node or a node with 2 or 3 children in ST(R). We define $v_i^{(l_i)}$ as the head node. If b is the number of children of parent of a head node and r is the number of revoked users in ST(R), then the maximum number of parent node is given by $\frac{r}{b}$ as each child belongs to a chain which contain at least one revoked user. Thus the number of chain at most $b\frac{r}{b}$. As each chain provides one subset cover, the number of cover is $b\frac{r}{b}$. Head of these chain will be new revoked users. This provides the maximum number of parent node to be $\frac{r}{b^2}$ as each branch from parent will contain at least one of the previous $\frac{r}{b}$ parent node (head of new revoked users). This generates cover size at most $b\frac{r}{b^2}$. Continue upto x th stage where $b^x = r$. So, we have an upper bound of the total number of subset cover as $b\frac{r}{b} + b\frac{r}{b^2} + \ldots + b\frac{r}{b^x}(b^x = r) = b(\frac{r}{b} + \frac{r}{b^2} + \ldots + \frac{r}{b^x}) = b\frac{r-1}{b-1}$. The root is an additional head vertex which provides one more to the cover, so total number of cover becomes $b\frac{r-1}{b-1} + 1$. This takes the maximum value at $b = 2$ and the value is $2r - 1$.

In terms of the total number of users N, the number of subsets will be at most $\frac{N}{3}$. This happens when all the subscribed users are covered by ternary tree of height 1. Again there are $N - r$ subscribers and cover partition subscribers

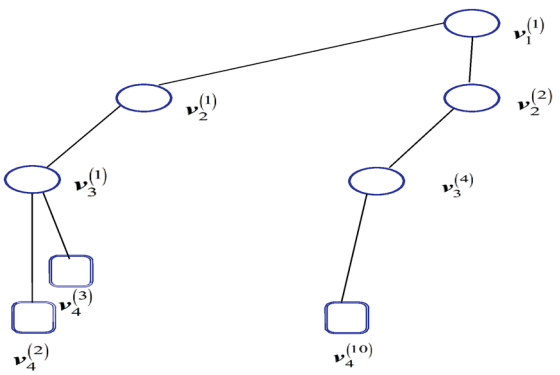

Fig. 4 Steiner Tree ST(R) for Fig. 3 where $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$

into groups. Therefore cover size should not exceed $N - r$. So, cover size $= \min\{\frac{N}{3}, N - r, 2r - 1\}$. □

Example We illustrate below the working of FindCover algorithm for the set of revoked users $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$. In Figure 3, $\mathsf{PN}(v_4^{(16)}) = \{v_1^{(1)}, v_2^{(2)}, v_3^{(6)}, v_4^{(16)}\}$ and $\mathsf{HN}(v_4^{(16)}) = \{v_2^{(1)}, v_2^{(3)}, v_3^{(4)}, v_3^{(5)}, v_4^{(17)}, v_4^{(18)}\}$. For the set of revoked users $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$, the Steiner tree $\mathsf{ST}(R)$ is depicted in Fig. 4. The Cover with respect to R is determined as follows:

(i) The chain C_1 corresponding to the revoked user $v_4^{(2)}$ (or $v_4^{(3)}$) is $v_2^{(1)}, v_3^{(1)}, v_4^{(2)}; v_4^{(3)}$, yielding the subset cover $S_{v_2^{(1)}, v_4^{(2)} + v_4^{(3)}}$.

(ii) The chain C_2 corresponding to the revoked user $v_4^{(10)}$ is $v_2^{(2)}, v_3^{(4)}, v_4^{(10)}$, yielding the subset cover $S_{v_2^{(2)}, v_4^{(10)}}$.

(iii) The head nodes $v_2^{(1)}$ and $v_2^{(2)}$ of the chains C_1, C_2 are then added to R. The nodes $v_4^{(2)}, v_4^{(3)}, v_4^{(10)}$ are removed from R and the chain corresponding to $v_2^{(1)}$ (or $v_2^{(2)}$) is $v_1^{(1)}, v_2^{(1)}; v_2^{(2)}$, yielding the set $S_{v_1^{(1)}, v_2^{(1)} + v_2^{(2)}}$.

(iv) Hence, $\mathsf{Cover} = S_{v_2^{(1)}, v_4^{(2)} + v_4^{(3)}} \cup S_{v_2^{(2)}, v_4^{(10)}} \cup S_{v_1^{(1)}, v_2^{(1)} + v_2^{(2)}}$.

Note that Cover is essentially a partition of the set of subscribed users into collection of disjoint subsets

$$S_{v_2^{(1)}, v_4^{(2)} + v_4^{(3)}} = \left\{ v_4^{(1)}, v_4^{(4)}, v_4^{(5)}, v_4^{(6)}, v_4^{(7)}, v_4^{(8)}, v_4^{(9)} \right\},$$

$$S_{v_2^{(2)}, v_4^{(10)}} = \left\{ v_4^{(11)}, v_4^{(12)}, v_4^{(13)}, v_4^{(14)}, v_4^{(15)}, v_4^{(16)}, v_4^{(17)}, v_4^{(18)} \right\},$$

$$S_{v_1^{(1)}, v_2^{(1)} + v_2^{(2)}} = \left\{ v_4^{(19)}, v_4^{(20)}, v_4^{(21)}, v_4^{(22)}, v_4^{(23)}, v_4^{(24)}, v_4^{(25)}, v_4^{(26)}, v_4^{(27)} \right\}.$$

4 Constructions

4.1 PKBE

Our *public key broadcast encryption* scheme PKBE= (Setup, KeyGeneration, Encrypt, Decrypt) enables a broadcaster to broadcast a message to a set of N users placed at the leaves of a complete ternary tree T. Let L be the level of the leaf nodes. The Setup and KeyGeneration algorithms are run by a trusted third party, called the Private Key Generation Center (PKGC), Encrypt algorithm is invoked by the broadcaster and Decrypt algorithm is carried out by the subscribed users. Formal description of these algorithms are provided in Algorithm 3–6.

High-level description Using the Setup algorithm, the PKGC generates the public and the master key. The PKGC keeps the master key private to itself and publishes the public key. A user at a leaf node receives the secret keys corresponding to all hanging node with respect to each path node from the PKGC by KeyGeneration algorithm through a secure communication channel between the PKGC and the subscribed user. The broadcaster runs FindCover procedure in Algorithm 2 and generates Cover (a partition of the subscribed users into disjoint subsets with respect to the set of revoked users). The KeyGeneration algorithm has a subroutine Derive which has 2 parts delegation and re-randomization. Delegation procedure helps to compute secret key of children using the secret key of its parent. Re-randomization helps to randomize the computed secret key. The broadcaster invokes Encrypt algorithm and forms the ciphertext components for each subset in Cover. The subscribed user u recovers the message from ciphertext components using the corresponding secret key.

Algorithm 3 Setup

input: Security parameter λ, total number of users N.
output: Public key parameter PK, master key MK.

1. Generate $\mathbb{S} = (n, \mathbb{G}, \mathbb{G}_T, e)$ using security parameter λ. Here $\mathbb{G}$ and $\mathbb{G}_\mathbb{T}$ are multiplicative cyclic groups of composite order $n = pq$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\mathbb{T}$ is a bilinear mapping. Let $\mathbb{G}_p, \mathbb{G}_q$ are subgroups of $\mathbb{G}$ with order p and q respectively and g_p, g_q are generators of $\mathbb{G}_p, \mathbb{G}_q$ respectively. One can take $g_p = g_1^q, g_q = g_1^p$, where g_1 is a generator of $\mathbb{G}$.
2. Choose random elements $g, f, v, h_1, \ldots, h_L, w$ from $\mathbb{G}_p$ and $R_g, R_f, R_v, R_1, \ldots, R_L$ from $\mathbb{G}_q$, where $L = \log_3 N + 1$ is the level of leaf nodes.
3. Compute $G = g.R_g, F = f.R_f, V = v.R_v, H_1 = h_1.R_1, \ldots, H_L = h_L.R_L, E = e(g, w)$.
4. The public key parameters are PK=$(g_p, g_q, G, F, V, H_1, H_2, \ldots, H_L, E, N, \mathbb{S})$.
5. The master key MK=$(p, q, g, f, v, h_1, h_2, \ldots, h_L, w)$.

Observe that public key and master key both are of size $O(L)$.

KeyGeneration algorithm (Algorithm 4) works as follows:

The PKGC generates the secret keys for all nodes in $\mathsf{HN}(v_L^{(l_L)})$ with respect to each node in $\mathsf{PN}(v_L^{(l_L)})$ and issues these keys to the subscribed user u at $v_L^{(l_L)}$. Let $sk_{u, v_i^{(l_i)}, v_j^{(l_j)}}$ denotes the secret key of the user u with respect to $v_j^{(l_j)} \in \mathsf{HN}(v_L^{(l_L)})$, $v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)})$, which corresponds to the identities $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_j)})$. Let $sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}}$ be the secret

keys of the user u corresponding to the identities $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j1})} + I_j^{(l_{j2})})$. Consider level 1 node $v_1^{(1)} \in \mathsf{PN}(v_L^{(l_L)})$. The PKGC uses step 2(a)i⟩ of Algorithm 4 to assign the secret keys corresponding to the nodes which are children of $v_1^{(1)}$. In this process, it gets the secret key of $v_2^{(l_2)} \in \mathsf{PN}(v_L^{(l_L)})$. The PKGC uses 2(a)ii⟩ to generate the combined secret key $sk_{u,v_1^{(1)},v_2^{(l_{j1})}+v_2^{(l_{j2})}}$, where $v_2^{(l_{j1})}, v_2^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})$. The PKGC uses Derive algorithm to derive the secret keys for nodes in $\mathsf{HN}(v_L^{(l_L)})$, that are not children of the initial path node $v_1^{(1)} \in \mathsf{PN}(v_L^{(l_L)})$. For example, the PKGC uses the secret key of $v_2^{(l_2)}$ to derive the secret keys for the children of $v_2^{(l_2)}$ (as in step 2(b)i⟩ of Algorithm 4). In this process, it gets secret key of $v_3^{(l_3)} \in \mathsf{PN}(v_L^{(l_L)})$. It uses 2(b)ii⟩ to generate the third level combined secret key of the form $sk_{u,v_1^{(1)},v_3^{(l_{j1})}+v_3^{(l_{j2})}}$, where $v_3^{(l_{j1})}, v_3^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})$. The PKGC uses the secret key of $v_3^{(l_3)} \in \mathsf{PN}(v_L^{(l_L)})$ to derive secret keys for the children of $v_3^{(l_3)}$ and continue up to level L-1 to obtain the secret key at leaf level. Next, consider level 2 node $v_2^{(l_2)} \in \mathsf{PN}(v_L^{(l_L)})$ and repeat the above process. Continue upto L-1 level node $v_{L-1}^{(l_{L-1})} \in \mathsf{PN}(v_L^{(l_L)})$. Finally, the user u at $v_L^{(l_L)}$ is issued the secret keys corresponding to all nodes in $\mathsf{HN}(v_L^{(l_L)})$ with respect to all nodes in $\mathsf{PN}(v_L^{(l_L)})$. The secret keys of user u is $sk_u = \{sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j2})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}} | 1 \le i \le L-1, i+1 \le j \le L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j1})}, v_j^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})\}$. As an example, in Fig. 3, user at $v_4^{(16)}$, will receive the secret key $sk_u = \Big\{ \{sk_{u,v_1^{(1)},v_2^{(x)}} | v_2^{(x)} = v_2^{(1)}, v_2^{(3)}, v_2^{(1)} + v_2^{(3)}\}, \{sk_{u,v_1^{(1)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_1^{(1)},v_4^{(z)}} | \ v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_2^{(2)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_2^{(2)},v_4^{(z)}} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_3^{(6)},v_4^{(z)}} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\} \Big\}$.

Algorithm 4 KeyGeneration

input: $(I_1^{(l_1)}, \ldots, I_L^{(l_L)})$, $\mathsf{PK}=(g_p, g_q, G, F, V, H_1, H_2, \ldots, H_L, E, N, \mathbb{S})$, $\mathsf{MK}=(p, q, g, f, v, h_1, h_2, \ldots, h_L, w)$

output: $sk_u = \{sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j2})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}} | 1 \le i \le L-1, i+1 \le j \le L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j1})}, v_j^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})\}$

1. ***for*** $i = 1$ to L-1 ***do***
   Let $v_i^{(l_i)} \in \mathsf{path}(v_L^{(l_L)})$
2. ***for*** $j = i+1$ to L ***do***
   for each $v_j^{(l_j)} \in \mathsf{HN}(v_L^{(l_L)}) \cup \mathsf{PN}(v_L^{(l_L)})$ ***do***
   (a) ***if*** $j = i+1$ ***then*** ▷ i.e., $v_j^{(l_j)}$ is a child of $v_i^{(l_i)}$
   i⟩ Note that, $v_j^{(l_j)}$ has the modified hierarchial identity $(I_i^{(l_i)}, I_{i+1}^{(l_{i+1})})$ with respect to $v_i^{(l_i)}$.
   – Take $r_1, r_2, s_1^{(1)}, s_2^{(1)}, s_1^{(2)}, s_2^{(2)} \in_R \mathbb{Z}_n$ such that $s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)} \not\equiv 0 \pmod q$, $s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)} \not\equiv 0 \pmod p$.
   – Compute

$$sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{j+1}^{r_1}, \ldots, h_L^{r_1}\Big)$$

$$sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(\big((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{s_1^{(x)}} f^{s_2^{(x)}}, g^{s_1^{(x)}}, g^{s_2^{(x)}}, h_{j+1}^{s_1^{(x)}}, \ldots, h_L^{s_1^{(x)}}\big)_{x=1,2}\Big).$$

$$\text{Set } sk_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}, sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}}\Big).$$

   ii⟩ Additionally, compute j-th level combined secret key $sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$ for identity $(I_i^{(l_i)}, I_j^{(l_{j1})} + I_j^{(l_{j2})})$ (as in 2(a)i⟩), where $v_j^{(l_{j1})}, v_j^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})$.
   end if
   (b) ***if*** $j \neq i+1$ ***then*** ▷ i.e., $v_j^{(l_j)}$ is not a child of $v_i^{(l_i)}$
   i⟩ Derive the secret keys $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$ from the secret key of upper level node $v_{i-1}^{(l_{i-1})} \in \mathsf{PN}(v_L^{(l_L)})$ using procedure Derive as described in Algorithm 9.
   ii⟩ Additionally, use procedure Derive to generate the j-th level combined secret key $sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$ for identity $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j1})} + I_j^{(l_{j2})})$, where $v_j^{(l_{j1})}, v_j^{(l_{j2})} \in \mathsf{HN}(v_L^{(l_L)})$.
   end if
   end for
3. ***end for***
4. ***return*** secret key sk_u to user u.

Secret key size The subscribed user at a leaf node gets the secret keys for all hanging node with respect to each path node. It gets 3 secret keys for height 1 path node, $3 \cdot 2$ secret keys for height 2 path node, $3 \cdot 3$ secret keys for height 3 path node and so on. Total number of secret keys of user u is given by $\sum_{k=1}^{\log_3 N} 3i = O(\log_3{}^2 N)$. Derive algorithm is a subroutine of KeyGeneration algorithm and used to derive secret key of child using the secret key of its parent. We have discussed this algorithm in appendix.

In encryption phase, the broadcaster divides the subscribed users into disjoint partitions using Find Cover and generates ciphertext components for each part.

Algorithm 5 Encrypt

input: Public key $\mathsf{PK}=(g_p, g_q, G, F, V, H_1, H_2, \ldots, H_L, E, N, \mathbb{S})$. $M \in \mathbb{G}_T$.
output: Ciphertext CT.

1. Find $\mathsf{Cover}=\{S_1, \ldots, S_m\}$ using Algorithm 2
   for $x = 1$ to m ***do***
   Let $S_x = S_{v_i^{(l_i)}, J} \in \mathsf{Cover}$.
   Let $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_j)})$ or $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j_1})}; I_j^{(l_{j_2})})$ be the node identity of the corresponding chain $(v_i^{(l_i)}, \ldots, v_j^{(l_j)})$ or $(v_i^{(l_i)}, \ldots, v_j^{(l_{j_1})}; v_j^{(l_{j_2})})$ of the subset cover $S_{v_i^{(l_i)}, J}$. Select Z_1, Z_2, Z_3 at random from $\mathbb{G}_q$, s at random from $\mathbb{Z}_n$.
   if $J = v_j^{(l_{j_1})} + v_j^{(l_{j_2})}$, ***then*** compute $C_x = \Big((M).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_1})} + I_j^{(l_{j_2})}})^s.Z_3\Big)$.
   if $J = v_j^{(l_{j_1})}$, ***then*** compute $C_x = \Big((M).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_1})}})^s.Z_3\Big)$.
   if $J = v_j^{(l_{j_2})}$, ***then*** compute $C_x = \Big((M).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_2})}})^s.Z_3\Big)$.
   end for
2. Set $C = \{C_1, C_2, \ldots, C_m\}$.
   Broadcast ciphertext $\mathsf{CT}=\{C\}$.

Remark Broadcaster can take $z_1 = g_q^{r_1}, z_2 = g_q^{r_2}, z_3 = g_q^{r_3}, r_1, r_2, r_3 \in_R \mathbb{Z}_n$. Components involving Z_1, Z_2, Z_3 are element of $\mathbb{G}$, so he can compute Z_1, Z_2, Z_3 on modulo n.

Ciphertext size Here ciphertext size = m, where m is the cover size.

Algorithm 6 Decrypt

input: PK, $\mathsf{CT}=\{C_1, C_2, \ldots, C_m\}$, $sk_u = \{sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_2})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}} | 1 \le i \le L-1, i+1 \le j \le L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$
output: Message M.

1. Run FindCover to find the cover in which user belongs,
2. Derive corresponding secret key $sk_{u, v_i^{(l_i)}, J}$.
3. Let a_0, a_1, a_2 be first 3 components of $sk^{(d)}_{u, v_i^{(l_i)}, J}$ extracted from $sk_{u, v_i^{(l_i)}, J}$.
   for ciphertext component $C_i = (\widehat{C}_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ ***do***
   Compute $M = \widehat{C}_1 \frac{e(a_1, \widehat{C}_4) e(a_2, \widehat{C}_3)}{e(a_0, \widehat{C}_2)}$
   return M.

Example In Fig. 3, $\mathsf{PN}(v_4^{(16)}) = \{v_1^{(1)}, v_2^{(2)}, v_3^{(6)}, v_4^{(16)}\}$ and $\mathsf{HN}(v_4^{(16)}) = \{v_2^{(1)}, v_2^{(3)}, v_3^{(4)}, v_3^{(5)}, v_4^{(17)}, v_4^{(18)}\}$, where the set of revoked user $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$. The user u at $v_4^{(16)}$, has the secret key $sk_u = \Big\{\{sk_{u,v_1^{(1)},v_2^{(x)}} | v_2^{(x)} = v_2^{(1)}, v_2^{(3)}, v_2^{(1)} + v_2^{(3)}\}, \{sk_{u,v_1^{(1)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_1^{(1)},v_4^{(z)}} | \ v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_2^{(2)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_2^{(2)},v_4^{(z)}} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_3^{(6)},v_4^{(z)}} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}\Big\}$. According to the Decrypt algorithm, the user will find cover $S_{v_1^{(1)},v_4^{(2)}+v_4^{(3)}}$, in which it belongs to. It will derive corresponding secret key $sk_{u,v_2^{(2)},v_4^{(10)}}$ and decrypt the ciphertext.

Correctnes: Using the fact that $e(h_p, h_q) = 1, h_p \in \mathbb{G}_p, h_q \in \mathbb{G}_q$, we show that ciphertext component $C_i = (\widehat{C}_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ generated for subset cover $S_{v_i^{(l_i)},v_j^{(l_j)}}$, will be decrypted using corresponding secret key $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$. Let a_0, a_1, a_2 are first 3 components of $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}$ extracted from $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$. Hence,

$$\begin{aligned}
&\widehat{C}_1 \frac{e(a_1, \widehat{C}_4)e(a_2, \widehat{C}_3)}{e(a_0, \widehat{C}_2)} \\
&= M.E^s \frac{e\left(g^{r_1}, (V.\prod_{k=i}^{j} H_k^{I_k^{(l_k)}})^s.Z_3\right).e(g^{r_2}, F^s.Z_2)}{e\left(w.\left(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^{r_1} f^{r_2}, G^s.Z_1\right)} \\
&= M.E^s \frac{e\left(g^{r_1}, (V.\prod_{k=i}^{j} H_k^{I_k^{(l_k)}})^s\right).e(g^{r_1}, Z_3).e(g^{r_2}, f^s).e(g^{r_2}, R_f{}^s.Z_2)}{e\left(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1} f^{r_2}, g^s\right)e(w.\left(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^{r_1} f^{r_2}, R_g{}^s.Z_1)} \\
&= M.E^s \frac{e\left(g^{r_1}, \left(v.\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^s\right).e(g^{r_2}, f^s)}{e(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1}.f^{r_2}, g^s)} \\
&= (M).E^s \frac{e\left(g^{r_1}, \left(v.\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^s\right).e(g^{r_2}, f^s)}{e\left(w.\left(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^{r_1}, g^s\right)e(f^{r_2}, g^s)} \\
&= M.E^s \frac{e\left(g^{r_1}, \left(v.\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^s\right)}{e\left(\left(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}}\right)^{r_1}, g^s\right)e(w, g^s)} = M.
\end{aligned}$$

Similarly, ciphertext component generated for the subset cover $S_{v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}$, can be decrypted by secret key $sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}$. In this case, $H_j^{I_j^{(l_j)}}$ is replaced by $H_j^{I_j^{(l_{j_1})}+I_j^{(l_{j_2})}}$.

Lemma 2 *The scheme PKBE attains revocation property.*

Proof When a user u at $v_L^{(l_L)}$ gets revoked, the cover changes. Let $v_L^{(l_L)} \in T_{v_i^{(l_i)}} \setminus S_{v_i^{(l_i)},v_j^{(l_j)}}$. Then $v_i^{(l_i)}$ will be ancestor of the node $v_L^{(l_L)}$ and $v_j^{(l_j)}$ will either itself be $v_L^{(l_L)}$ or will be an ancestor of $v_L^{(l_L)}$. If $v_j^{(l_j)}$ is not an ancestor of $v_L^{(l_L)}$, then $v_L^{(l_L)}$ cannot be a revoked user as in $S_{v_i^{(l_i)},v_j^{(l_j)}}$, users at the leaf of the complete subtree rooted at $v_j^{(l_j)}$ are the revoked users. Thus both $v_i^{(l_i)}, v_j^{(l_j)} \in \mathsf{PN}(v_L^{(l_L)})$. As the user has the secret keys $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$, where $v_j^{(l_j)} \in \mathsf{HN}(v_L^{(l_L)})$, it will be unable to recover the message from the ciphertext generated corresponding to new Cover. □

Lemma 2 shows that users who have not subscribed (i.e., revoked users) should not be able to recover the message. It is true for any number of revoked users thus independent of cover size. Hence independent of communication bandwidth and computation cost.

Example In Fig. 3, $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$ is the set of revoked users. Revoked user $v_4^{(10)}$ has secret key $sk_u = \Big\{\{sk_{u,v_1^{(1)},v_2^{(x)}} | v_2^{(x)} = v_2^{(1)}, v_2^{(3)}, v_2^{(1)} + v_2^{(3)}\}, \{sk_{u,v_1^{(1)},v_3^{(y)}} | v_3^{(y)} = v_3^{(6)}, v_3^{(5)}, v_3^{(6)} + v_3^{(5)}\}, \{sk_{u,v_1^{(1)},v_4^{(z)}} | \quad v_4^{(z)} = v_4^{(11)}, v_4^{(12)}, v_4^{(11)} + v_4^{(12)}\}, \{sk_{u,v_2^{(2)},v_3^{(y)}} | v_3^{(y)} = v_3^{(6)}, v_3^{(5)}, v_3^{(6)} + v_3^{(5)}\}, \{sk_{u,v_2^{(2)},v_4^{(z)}} | v_4^{(z)} = v_4^{(11)}, v_4^{(12)}, v_4^{(11)} + v_4^{(12)}\}, \{sk_{u,v_3^{(4)},v_4^{(z)}} | v_4^{(z)} = v_4^{(11)}, v_4^{(12)}, v_4^{(11)} + v_4^{(12)}\}\Big\}$. The set of revoked users $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$ generates subset difference $\mathsf{Cover} = S_{v_2^{(1)},v_4^{(2)}+v_4^{(3)}} \cup S_{v_2^{(2)},v_4^{(10)}} \cup S_{v_1^{(1)},v_2^{(1)}+v_2^{(2)}}$. Secret key required for decryption are $sk_{u,v_2^{(1)},v_4^{(2)}+v_4^{(3)}}, sk_{u,v_2^{(2)},v_4^{(10)}}, sk_{u,v_1^{(1)},v_2^{(1)}+v_2^{(2)}}$ respectively. Derive algorithm (see Appendix) only helps to derive secret key of child using the secret key of its parent. As the revoked user does not have decryption key corresponding to the ciphertext components, will not able to recover the message.

- *Security analysis*

Theorem 1 *The construction PKBE achieves selective semantic security under L-wDBDHI* assumptions.*

Proof Let there is an adversary $\mathcal{A}$ that can distinguish win the game with an advantage ϵ. We show that $\mathcal{C}$ can solve L-wDBDHI* problem with advantage ϵ. Challenger $\mathcal{C}$ has input L-wDBDHI* instance $Z = (\mathbb{S}, h, g_q, g_p, g_p^{\alpha}, \ldots, g_p^{\alpha^L}), T$, where $h \in_R \mathbb{G}_p, \alpha \in_R \mathbb{Z}_n, T \in_R \mathbb{G}_{T,p}, \mathbb{S} = (n, \mathbb{G}, \mathbb{G}_T, e)$.

1. Initialization: $\mathcal{A}$ submits the challenge revoked sets $\mathbb{R}$ to $\mathcal{C}$.
2. Setup: $\mathcal{C}$ chooses $\gamma, x, y, z, x_1, \ldots, x_L \in_R \mathbb{Z}_n$ and $R_g, R_f, R_v, R_{h,1}, \ldots, R_{h,L} \in_R \mathbb{G}_q$. Let us consider a cover $S_{v_i^{(\bar{l}_i)},v_j^{(\bar{l}_j)}}$ generated by the chain $(v_i^{(\bar{l}_i)}, v_{i+1}^{(\bar{l}_{i+1})}, \ldots, v_j^{(\bar{l}_j)})$, using

the revoked set $\mathbb{R}_0$. Let modified hierarchial identity of the end node $v_j^{(\bar{l}_j)}$ with respect to the head node $v_i^{(\bar{l}_i)}$ as

$$\left(0,\ldots,0,I_i^{(\bar{l}_i)},I_{i+1}^{(\bar{l}_{i+1})},\ldots,I_j^{(\bar{l}_j)},0,\ldots,0\right)$$
$$=\left(I_1^{(\bar{l}_1)},I_2^{(\bar{l}_2)},\ldots,I_L^{(\bar{l}_L)}\right).$$

So, some $I_k^{(\bar{l}_k)}$ may be 0 at the beginning and end. Compute $G=g_p.R_g, F=g_p^z.R_f, V=g_p^y.\prod_{k=1}^{L}(A_{L-k+1})^{I_k^{(\bar{l}_k)}}R_v$, $H_k=g_p^{x_k}/A_{L-k+1}R_{h,k}$ $(1\le k\le L)$, $E=e(A_1,A_Lg_p^{\gamma})$, where $A_k=g_p^{\alpha^k}$. Set public key as $\mathsf{PK}=(g_p,g_q,G,F,V,H_1,\ldots,H_L,E,N,\mathbb{S})$ and $w=(A_Lg_p^{\gamma})^{\alpha}=A_{L+1}A_1^{\gamma}$. Challenger does not have A_{L+1}, so he cannot compute w explicitly.

3. Phase 1: Let $\mathcal{A}$ wants to get secret keys for revoked user $i\in\mathbb{R}$. Let i be in $T_{v_j^{(l_j)}}$ of cover $S_{v_i^{(l_i)},v_j^{(l_j)}}$ and it queries for a secret key component corresponding to modified hierarchial identity $(I_1^{(l_1)^*},I_2^{(l_2)^*},\ldots,I_L^{(l_L)^*})$. Let s be the least identity such that $I_s^{(\bar{l}_s)}\ne I_s^{(l_s)^*}$.

i. Take $r_1,r_2\in_R\mathbb{Z}_n$ and implicitly set $\bar{r}_1=r_1+\frac{\alpha^s}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}$. Secret key $g,f,v,h_1,\ldots,h_L$ can be obtained by removing the blinding factors $R_g,R_f,R_v,R_{h,1},\ldots,R_{h,L}$ from $G,F,V,H_1,\ldots,H_L$ respectively.

ii. Next, $\mathcal{C}$ tries to compute

$$w.\left(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}}\right)^{\bar{r}_1}f^{r_2}=w.\left(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}}\right)^{r_1}f^{r_2}.\left(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}.$$

Using secret keys v,h_k $(1\le k\le s)$, f and public value $I_k^{(l_k)^*}$ $(1\le k\le s)$, $(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}})^{r_1}f^{r_2}$ is computable. Now,

$$w.\left(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}$$
$$=A_{L+1}A_1^{\gamma}\left(g_p^y.\prod_{k=1}^{L}(A_{L-k+1})^{I_k^{(\bar{l}_k)}}\prod_{k=1}^{s}(g_p^{x_k}/A_{L-k+1})^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}$$
$$=A_{L+1}A_1^{\gamma}\left(A_{L+1}^{I_s^{(\bar{l}_s)}-I_s^{(l_s)^*}}.A_s^y.\prod_{k=s+1}^{L}(A_{L+s-k+1})^{I_k^{(\bar{l}_k)}}\prod_{k=1}^{s}A_s^{x_k.I_k^{(l_k)^*}}\right)^{\frac{1}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}$$
$$=A_1^{\gamma}\left(A_s^y.\prod_{k=s+1}^{L}(A_{L+s-k+1})^{I_k^{(\bar{l}_k)}}\prod_{k=1}^{s}A_s^{x_k.I_k^{(l_k)^*}}\right)^{\frac{1}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}.$$

As $A_k,I_k^{(l_k)^*},x_k$ values are available, $w.(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}})^{\frac{\alpha^s}{I_s^{(l_s)^*}-I_s^{(\bar{l}_s)}}}$ is computable, so $w.(v\prod_{k=1}^{s}h_k^{I_k^{(l_k)^*}})^{\bar{r}_1}$. f^{r_2} is also computable.

iii. Now using Derive algorithm as stated in Algorithm 9, $\mathcal{C}$ computes first component of $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ as $w.(v\prod_{k=1}^{j}h_k^{I_k^{(l_k)^*}})^{\bar{r}_1}f^{r_2}$. Other components $(g^{\bar{r}_1},g^{r_2},h_{j+1}^{\bar{r}_1},\ldots,h_L^{\bar{r}_1})$ of $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ are easily computable using secret key components.

iv. Challenger need to choose $s_1^{(1)},s_2^{(1)},s_1^{(2)},s_2^{(2)}\in_R\mathbb{Z}_n$ such that $s_1^{(1)}s_2^{(2)}-s_2^{(1)}s_1^{(2)}\not\equiv 0\pmod q$, $s_1^{(1)}s_2^{(2)}-s_2^{(1)}s_1^{(2)}\not\equiv 0\pmod p$, for this it check the equation $g_p^{s_1^{(1)}s_2^{(2)}-s_2^{(1)}s_1^{(2)}}\not\equiv 1$ and $g_q^{s_1^{(1)}s_2^{(2)}-s_2^{(1)}s_1^{(2)}}\not\equiv 1$. Components of $sk^{(r)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ are almost same with $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ except first component does not contain w. So, $\mathcal{C}$ computes $sk^{(r)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ as previous. Similarly, it can generate secret key $sk_{i,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$.

v. Adversary gets $sk_i=\{sk_{i,v_i^{(l_i)},v_j^{(l_{j1})}},sk_{i,v_i^{(l_i)},v_j^{(l_{j2})}},sk_{i,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}\}$, where user i is at $v_L^{(l_L)}$ and $v_i^{(l_i)}\in\mathsf{PN}(v_L^{(l_L)}),v_j^{(l_{j1})},v_j^{(l_{j2})}\in\mathsf{HN}(v_L^{(l_L)})$.

4. Challenge: $\mathcal{A}$ sends two messages m_0,m_1 to $\mathcal{C}$. $\mathcal{C}$ computes ciphertext components $\{C_1,\ldots,C_{l_0}\}$ following Algorithm 5 as follows.

$$C_i=\left(m_0.T.e(A_1,h^{\gamma}),h.Z_1,h^z.Z_2,h^{y+\sum_{k=1}^{L}I_k^{(l_k)}.x_k}.Z_3\right),$$
$$1\le i\le l_0$$
where $Z_1,Z_2,Z_3\in_R\mathbb{G}_q, s\in_R\mathbb{Z}_n, T\in_R\mathbb{G}_{T,p}$.

$\mathcal{C}$ sends ciphertext $\{C_1,\ldots,C_{l_0}\}$ to $\mathcal{A}$. As g_p is generator for $\mathbb{G}_p$, let us consider $h=g_p{}^c$, for some integer c. If $T=e(g_p,g_p{}^c)^{\alpha^{L+1}}$ then ciphertext component

$$C_i=\left(m_0.e(g_p,g_p{}^c)^{\alpha^{L+1}}.e(A_1,h^{\gamma}),\right.$$
$$\left.h.Z_1,h^z.Z_2,h^{y+\sum_{k=1}^{L}I_k^{(l_k)}.x_k}.Z_3\right)$$
where $Z_1,Z_2,Z_3\in\mathbb{G}_q$.
$$=\left(m_0.E^c,G^c.Z_1',F^c.Z_2',(V\prod_{k=1}^{L}H_k^{I_k^{(l_k)}})^c.Z_3'\right)$$

This implies, if $T=e(g_p,g_p{}^c)^{\alpha^{L+1}}$ then ciphertext $\{C_1,\ldots,C_{l_0}\}$ is identical with original.

5. Phase 2: Same as Phase 1.
6. Guess: $\mathcal{A}$ predicts b' for b and wins the game if $b'=b$.

Adversary's advantage of winning the game is same as deciding $T=e(g_p,g_p{}^c)^{\alpha^{L+1}}$ or not, i.e., solving L-wDBDHI* problem. □

4.2 OAnoBE

In this section, we will discuss our outsider anonymous broadcast encryption scheme OAnoBE which is an extension of our PKBE. In PKBE each user gets a set of keys.

The keys are helpful to recover secret key corresponding to the subset cover in which it belongs. Thus a user can try to decrypt the ciphertext by using the possible subset cover in which it belongs without knowing the set of subscribers or revoked users. Hence PKBE can be extended to develop an anonymous construction, namely OAnoBE. OAnoBE works similar to PKBE, except encryption and decryption. We will explain these two algorithms as follows:

The encryption algorithm works as follows: The broadcaster encrypts $M\|K$ instead of M in encryption algorithm. Here K is the verification component. It computes l components where components $\{C_x\}_{x=m+1}^{l}$ are random and $\{C_x\}_{x=1}^{m}$ are same as PKBE. Here l is the theoretical upper bound of cover size and m is cover size. The detail description as follows:

Algorithm 7 Encrypt

input: Public key $\mathsf{PK}=(g_p, g_q, G, F, V, H_1, H_2, \ldots, H_L, E, N, \mathbb{S})$, $l=\min\{\frac{N}{3}, N-r, 2r-1\}$, r is number of revoked users. $(M\|K) \in \mathbb{G}_T$, where $M \in \{0,1\}^{\lambda-k}$ is the message and $K \in \{0,1\}^k$ is the verification component.
output: Ciphertext CT.

1. Find $\mathsf{Cover}=\{S_1, \ldots, S_m\}$ using Algorithm 2
2. ***for*** $i = 1$ to l
   (a) ***for*** $x = 1$ to m ***do***
   Let $S_x = S_{v_i^{(l_i)}, J} \in \mathsf{Cover}$.
   Let $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_j)})$ or $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j_1})}; I_j^{(l_{j_2})})$ be the node identity of the corresponding chain $(v_i^{(l_i)}, \ldots, v_j^{(l_j)})$ or $(v_i^{(l_i)}, \ldots, v_j^{(l_{j_1})}; v_j^{(l_{j_2})})$ of the subset cover $S_{v_i^{(l_i)}, J}$. Select Z_1, Z_2, Z_3 at random from $\mathbb{G}_q$, s at random from $\mathbb{Z}_n$.

   if $J = v_j^{(l_{j_1})} + v_j^{(l_{j_2})}$, ***then*** compute $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_1})} + I_j^{(l_{j_2})}})^s.Z_3\Big)$.

   if $J = v_j^{(l_{j_1})}$, ***then*** compute $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_1})}})^s.Z_3\Big)$.

   if $J = v_j^{(l_{j_2})}$, ***then*** compute $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j_2})}})^s.Z_3\Big)$.

   end for
   (b) ***for*** $x = m+1$ to l ***do***
   Choose $R_1 \in_R \mathbb{G}_T, R_2, R_3, R_4 \in_R \mathbb{G}$.
   Set $C_x = (R_1, R_2, R_3, R_4)$.
   end for
3. ***end for***
4. Set $C = \{C_1, C_2, \ldots, C_l\}$.
   Use permutation μ to compute $C_\mu = \{C_{\mu(1)}, C_{\mu(2)}, ..C_{\mu(l)}\}$.
   Broadcast ciphertext $\mathsf{CT}=\{k, K, C_\mu\}$.

Remark Broadcaster can take $Z_1 = g_q^{r_1}, Z_2 = g_q^{r_2}, Z_3 = g_q^{r_3}, r_1, r_2, r_3 \in_R \mathbb{Z}_n$. Components involving Z_1, Z_2, Z_3 are element of $\mathbb{G}$, so he can compute Z_1, Z_2, Z_3 on modulo n.

Ciphertext size Here ciphertext size = $l=\min\{\frac{N}{3}, N-r, 2r-1\}$.

The broadcaster invokes Encrypt algorithm and forms the ciphertext components for each subset in Cover. To preserve the anonymity, the broadcaster also generates $(l - |Cover|)$ many dummy ciphertext components, where l is theoretical bound of cover size. The decryption algorithm works as follows:

Algorithm 8 Decrypt

input: PK, CT=$\{k, K, C_\mu\}$, $sk_u = \{sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_2})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}} | 1 \le i \le L-1, i+1 \le j \le L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$

output: Message $M \in \{0,1\}^{\lambda-k}$.

1. ***for*** $i = 1$ to L-1 ***do***
   Let $v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)})$.
2. ***for*** $j = i+1$ to L ***do***
   Let $v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})$.
   Set $J = v_j^{(l_{j_1})} + v_j^{(l_{j_2})}$.
3. Let a_0, a_1, a_2 be first 3 components of $sk^{(d)}_{u,v_i^{(l_i)},J}$ extracted from $sk_{u,v_i^{(l_i)},J}$.
   for each ciphertext component $C_i = (\widehat{C}_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ ***do***
   Compute $M^\star = \widehat{C}_1 \frac{e(a_1,\widehat{C}_4)e(a_2,\widehat{C}_3)}{e(a_0,\widehat{C}_2)}$
   if last k bits of $M^\star$ matches with K ***then***
   return first $\{\lambda - k\}$ bits as M.
   else
   (a) ***for*** each hanging node $v_j^{(l_j)}$ (i.e., $v_j^{(l_{j_1})}$ or $v_j^{(l_{j_2})}$) ***do***
   Set $J = v_j^{(l_j)}$ and execute initial 5 lines of step 3.
   if M is not recovered ***then***
   for $k = j+1$ to L ***do***
   i⟩ sequentially set $J = v_k^{(l_k)}$, where $v_k^{(l_k)}$ is the k-th level node in $T_{v_j^{(l_j)}}$. Compute the secret key $sk_{u,v_i^{(l_i)},J}$ using the delegation mechanism of algorithm Derive. Execute first 5 lines of step 3 until M is recovered.
   ii⟩ sequentially set $J = v_k^{(l_{k_1})} + v_k^{(l_{k_2})}$, where $v_k^{(l_{k_1})}, v_k^{(l_{k_2})}$ are the k-th level siblings in $T_{v_j^{(l_j)}}$. Compute the combined secret key $sk_{u,v_i^{(l_i)},J}$ using the delegation mechanism of algorithm Derive. Execute first 5 lines of step 3 until M is recovered.
   end for
   end if
   end for
   (b) ***end for***
   end if
   end for
4. ***end for***
5. ***end for***

Decryption attempt To recover the message using Decrypt algorithm, user u tries to decrypt $\{C_i\}_{i=1}^{l}$ values with secret key corresponds to all possible subsets in which it can belong to. For height k, there are at most $2 \cdot 3$ subsets of depth 1, $2 \cdot 3^2$ of depth 2 and so on. So, total $2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^k$ subsets. But, the user does not belong to $3k$ subsets of the form $S_{v_i^{(l_i)},v_j^{(l_j)}}$,$S_{v_i^{(l_i)},v_j^{(l_j)}+v_j^{(l'_j)}}$, where $v_j^{(l_j)}$ lies on the path joining the user and the root. So, for height k, the user can belong to $2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^k - 3k = 3 \cdot (3^k - 1) - 3k \le 3^{k+1} - 3k$ subset difference sets. This gives the maximum number of subsets in which it can belong, is $\sum_{k=1}^{\log_3 N} (3^{k+1} - 3k) = O(N)$. The user generates or derive secret keys for each subsets and decrypt l ciphertext components one by one until it recover message M. So, total number of decryption attempt is $O(Nl)$.

Example In Fig. 3, $\mathsf{PN}(v_4^{(16)}) = \{v_1^{(1)}, v_2^{(2)}, v_3^{(6)}, v_4^{(16)}\}$ and $\mathsf{HN}(v_4^{(16)}) = \{v_2^{(1)}, v_2^{(3)}, v_3^{(4)}, v_3^{(5)}, v_4^{(17)}, v_4^{(18)}\}$, where the set of revoked user $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$. The user u at $v_4^{(16)}$, has the secret key $sk_u = \Big\{ \{sk_{u,v_1^{(1)},v_2^{(x)}} | v_2^{(x)} = v_2^{(1)}, v_2^{(3)}, v_2^{(1)} + v_2^{(3)}\}, \{sk_{u,v_1^{(1)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_1^{(1)},v_4^{(z)}} | \ v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_2^{(2)},v_3^{(y)}} | v_3^{(y)} = v_3^{(4)}, v_3^{(5)}, v_3^{(4)} + v_3^{(5)}\}, \{sk_{u,v_2^{(2)}}, v_4^{(z)} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, \ v_4^{(17)} + v_4^{(18)}\}, \{sk_{u,v_3^{(6)},v_4^{(z)}} | v_4^{(z)} = v_4^{(17)}, v_4^{(18)}, v_4^{(17)} + v_4^{(18)}\} \Big\}$. According to the Decrypt algorithm, the user will try to decrypt the ciphertext using the secret keys $sk_{u,v_1^{(1)},v_2^{(1)}+v_2^{(3)}}$, $sk_{u,v_1^{(1)},v_2^{(1)}}$ respectively and will fail to recover the message as no ciphertext components corresponding to the subset cover $S_{v_1^{(1)},J}, J = v_2^{(1)}, v_2^{(1)} + v_2^{(3)}$. If user has the secret key $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$ for $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})})$, then it can compute the secretkeys $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$, $sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}$ for

$(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_j)}), (I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j_1})} + I_j^{(l_{j_2})})$ by the delegation mechanism of Derive. Using this mechanism, subscribed user u will compute the following 3-rd level keys which belong to $T_{v_2^{(1)}}$: the individual secret keys $sk_{u,v_1^{(1)},v_3^{(1)}}$, $sk_{u,v_1^{(1)},v_3^{(2)}}$, $sk_{u,v_1^{(1)},v_3^{(3)}}$ and the combined secret keys $sk_{u,v_1^{(1)},v_3^{(1)}+v_3^{(2)}}$, $sk_{u,v_1^{(1)},v_3^{(2)}+v_3^{(3)}}$, $sk_{u,v_1^{(1)},v_3^{(1)}+v_3^{(3)}}$. User u will try with these keys and and fail to recover the message. User u will compute the following fourth level individual secret keys in $T_{v_2^{(1)}}$: $sk_{u,v_1^{(1)},v_4^{(1)}}$, $sk_{u,v_1^{(1)},v_4^{(2)}}$, $sk_{u,v_1^{(1)},v_4^{(3)}}$ and still be unable to recover the message. It succeeds with the combined secret key $sk_{u,v_1^{(1)},v_4^{(2)}+v_4^{(3)}}$ as there is a ciphertext component generated for $S_{v_1^{(1)},v_4^{(2)}+v_4^{(3)}}$.

- *Security analysis* The security works similar to the PKBE scheme. We explain the security in detail.

Theorem 2 *The scheme OAnoBE scheme described in Sect. 4 is selective secure against CPA under L-wDBDHI*, BSD and L-cDDH assumptions, where L is the level of leaf nodes.*

Proof We will organize the proof in a sequence of games: $\mathsf{Game}_h^0 \quad (0 \le h < l_0), \mathsf{Game}_{l_0}^0, \mathsf{Game}_{l_1}^1, \mathsf{Game}_k^1 \quad (l_1 > k \ge 1)$ played between challenger $\mathcal{C}$ and adversary $\mathcal{A}$, where l_i, $(i = 0, 1)$ is the cover size generated for the revoked set $\mathbb{R}_i$. Let the i-th chain of $\mathsf{ST}(\mathbb{R}_0)$ contains nodes $(v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_j)})$. As $\mathbb{R}_0, \mathbb{R}_1$ has equal number of revoked users, theoretical bound of cover size $l_1 = l_2 = l$ (say). Let $(I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)})$ be the modified hierarchial identity of the last node $v_j^{(l_j)}$ of i-th chain with respect to its head node $v_i^{(l_i)}$. If the i-th chain of $\mathsf{ST}(\mathbb{R}_0)$ contains nodes $(v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_{j_1})}; v_j^{(l_{j_2})})$, then the modified hierarchial identity is $(I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_{j_1})} + I_j^{(l_{j_2})})$. Let

$$\begin{aligned}\mathsf{ID}_{i,0} &= \left(0, \ldots, 0, I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)}, 0, \ldots, 0\right) \\ &= \left(I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_L^{(l_L)}\right).\end{aligned}$$

We start with the first game Game_0^0 where the challenger encrypts $m_0 = (M_0||K)$ for the adversary's challenge revoked set $\mathbb{R}_0$. We then gradually change the encryption through multiple games into encryption of $m_1 = (M_1||K)$ for the revoked set $\mathbb{R}_1$. We show that each game is indistinguishable from its previous one. Thus showing our OAnoBE scheme to have selective security against CPA.

– $\mathsf{Game}_h^0 (0 \le h < l_0)$:

1. Initialization: Adversary $\mathcal{A}$ sends the challenge sets $\mathbb{R}_0, \mathbb{R}_1$ to $\mathcal{C}$, where $\mathbb{R}_0, \mathbb{R}_1$ have equal number of revoked users.
2. Setup: $\mathcal{C}$ runs $(\mathsf{PK}, \mathsf{MK}) \leftarrow \mathsf{Setup}(N, \lambda)$. It keeps MK secret to itself and makes PK public.
3. Phase 1: $\mathcal{A}$ takes an user $i \in \mathbb{R}_0 \cap \mathbb{R}_1$ and requests for the secret keys to $\mathcal{C}$. $\mathcal{C}$ generates the secret key $sk_i \leftarrow \mathsf{KeyGeneration}(\mathsf{PK}, \mathsf{MK}, i)$ and sends to $\mathcal{A}$.
4. Challenge: $\mathcal{A}$ sends two equal length messages $m_0 = (M_0||K)$, $m_1 = (M_1||K)$, where last k bits of each message is K. $\mathcal{C}$ computes following ciphertext components: C_i, $1 \le i \le l_0 - h$ as encryption of m_0 for identity $\mathsf{ID}_{i,0}$ and C_i, $l_0 - h + 1 \le i \le l$ as $(R_1, R_2, R_3, R_4) \in_R \mathbb{G}_T \times \mathbb{G}^3$ following Algorithm 7. $\mathcal{C}$ permutes the C_i values using some permutation μ and sends $\{k, K, C_{\mu(1)}, \ldots, C_{\mu(l)}\}$ to $\mathcal{A}$.
5. Phase 2: Phase 2 is similar to Phase 1.
6. Guess: $\mathcal{A}$ wins the game if he can predict $b = 0$.

– $\mathsf{Game}_{l_0}^0$: This game is similar to above except that challenge ciphertext component $C_i, 1 \le i \le l$ as $(R_1, R_2, R_3, R_4) \in_R \mathbb{G}_T \times \mathbb{G}^3$ following Algorithm 7. Let us now consider that the i-th chain of $\mathsf{ST}(\mathbb{R}_1)$ contains nodes $(v_i^{(l_i)}, v_{i+1}^{(l_{i+1})}, \ldots, v_j^{(l_j)})$ and $(I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)})$ be the modified hierarchial identity of the last node $v_j^{(l_j)}$ of this chain with respect to its head node $v_i^{(l_i)}$. Let $\mathsf{ID}_{i,1} = (0, \ldots, 0, I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)}, 0, \ldots, 0) = (I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_L^{(l_L)})$.

– $\mathsf{Game}_{l_1}^1$: This game is identical to $\mathsf{Game}_{l_0}^0$.

– Game_k^1 $(l_1 > k \ge 1)$: This game continues as in $\mathsf{Game}_{l_1}^1$ except that the challenge ciphertext components. $\mathcal{A}$ sends two equal length messages $m_0 = (M_0||K), m_1 = (M_1||K)$. $\mathcal{C}$ computes following ciphertext components: C_i, $1 \le i \le l_1 - k$ as encryption of m_1 for identity $\mathsf{ID}_{i,1}$ and C_i, $l_1 - k + 1 \le i \le l$ as $(R_1, R_2, R_3, R_4) \in_R \mathbb{G}_T \times \mathbb{G}^3$ following Algorithm 7. $\mathcal{C}$ permutes the C_i values using some permutation μ and sends $\{k, K, C_{\mu(1)}, \ldots, C_{\mu(l)}\}$ to $\mathcal{A}$.

We now present a sequence of lemmas which will demonstrate that no PPT adversary can distinguish with non-negligible advantage between any two consecutive game described above. In Lemma 3, we show that Game_{h-1}^0 and Game_h^0, $1 \le h \le l_0$ are indistinguishable if L-wDBDHI*, BSD and L-cDDH assumption holds. Game_{k-1}^1 and Game_k^1, $2 \le k \le l_1$ are indistinguishable by Lemma 4 under the same assumptions. Let the adversary's advantage of winning Game_h^0 is Adv_h^0, and that of Game_k^1 is Adv_k^1. Let the adversary's advantage of distinguishing Game_h^0, Game_{h-1}^0 and Game_k^0, Game_{k-1}^0 is at most ϵ. Then advantage of distinguishing Game_0^0, Game_1^1 is given by

$$|\mathsf{Adv}_0^0 - \mathsf{Adv}_1^1| \le \sum_{h=1}^{l_0} |\mathsf{Adv}_{h-1}^0 - \mathsf{Adv}_h^0| + |\mathsf{Adv}_{l_0}^0 - \mathsf{Adv}_{l_1}^1| + \sum_{k=2}^{l_1} |\mathsf{Adv}_k^1 - \mathsf{Adv}_{k-1}^1| \le \epsilon(l_0 + l_1) \le \epsilon(l + l) \le 2\epsilon(l).$$

□

Lemma 3 Game_{h-1}^0 and Game_h^0 *are indistinguishable under L-wDBDHI*, BSD and L-cDDH assumptions*.

Proof To prove the indistinguishability of Game_{h-1}^0 and Game_h^0, we define $\overline{\mathsf{Game}}_h^0$ in slightly different way from Game_h^0 and prove the indistinguishability of $\overline{\mathsf{Game}}_{h-1}^0$ and $\overline{\mathsf{Game}}_h^0$. For $i = l_0 - h + 1$ to l, the generated challenged ciphertext in $\overline{\mathsf{Game}}_h^0$ is of the form $(\widehat{C}_1.R_p, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ instead of $(R_1, R_2, R_3, R_4) \in_R \mathbb{G}_T \times \mathbb{G}^3$, where $(\widehat{C}_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ is the encryption of the message m_0 using $\mathsf{ID}_{i,0}$ and $R_p \in_R \mathbb{G}_{T,p}$.

Claim. $\overline{\mathsf{Game}}_{h-1}^0$ and $\overline{\mathsf{Game}}_h^0$ are indistinguishable under L-wDBDHI* assumptions.

Proof. Let there is an adversary $\mathcal{A}$ that can distinguish $\overline{\mathsf{Game}}_{h-1}^0$ and $\overline{\mathsf{Game}}_h^0$ with an advantage ϵ. We show that $\mathcal{C}$ can solve L-wDBDHI* problem with advantage ϵ. Challenger $\mathcal{C}$ has input L-wDBDHI* instance $Z = (\mathbb{S}, h, g_q, g_p, g_p^\alpha, \ldots, g_p^{\alpha^L}), T$, where $h \in_R \mathbb{G}_p, \alpha \in_R \mathbb{Z}_n, T \in_R \mathbb{G}_{T,p}, \mathbb{S} = (n, \mathbb{G}, \mathbb{G}_T, e)$.

1. Initialization: $\mathcal{A}$ submits the challenge revoked sets $\mathbb{R}_0, \mathbb{R}_1$ to $\mathcal{C}$, where $\mathbb{R}_0, \mathbb{R}_1$ has equal number of revoked users.
2. Setup: $\mathcal{C}$ chooses $\gamma, x, y, z, x_1, \ldots, x_L \in_R \mathbb{Z}_n$ and $R_g, R_f, R_v, R_{h,1}, \ldots, R_{h,L} \in_R \mathbb{G}_q$. Let us consider a cover $S_{v_i^{(\bar{l}_i)}, v_j^{(\bar{l}_j)}}$ generated by the chain $(v_i^{(\bar{l}_i)}, v_{i+1}^{(\bar{l}_{i+1})}, \ldots, v_j^{(\bar{l}_j)})$, using the revoked set $\mathbb{R}_0$. Let modified hierarchial identity of the end node $v_j^{(\bar{l}_j)}$ with respect to the head node $v_i^{(\bar{l}_i)}$ as
$$\left(0, \ldots, 0, I_i^{(\bar{l}_i)}, I_{i+1}^{(\bar{l}_{i+1})}, \ldots, I_j^{(\bar{l}_j)}, 0, \ldots, 0\right) = \left(I_1^{(\bar{l}_1)}, I_2^{(\bar{l}_2)}, \ldots, I_L^{(\bar{l}_L)}\right).$$
So, some $I_k^{(\bar{l}_k)}$ may be 0 at the beginning and end. Compute $G = g_p.R_g, F = g_p^z.R_f, V = g_p^y.\prod_{k=1}^{L}(A_{L-k+1})^{I_k^{(\bar{l}_k)}} R_v$, $H_k = g_p^{x_k}/A_{L-k+1}R_{h,k}\ (1 \le k \le L)$, $E = e(A_1, A_L g_p^\gamma)$, where $A_k = g_p^{\alpha^k}$. Set public key as $\mathsf{PK} = (g_p, g_q, G, F, V, H_1, \ldots, H_L, E, N, \mathbb{S})$ and $w = (A_L g_p^\gamma)^\alpha = A_{L+1}A_1^\gamma$. Challenger does not have A_{L+1}, so he cannot compute w explicitly.
3. Phase 1: Let $\mathcal{A}$ wants to get secret keys for revoked user $i \in \mathbb{R}_0 \cap \mathbb{R}_1$. Let i be in $T_{v_j^{(\bar{l}_j)}}$ of cover $S_{v_i^{(\bar{l}_i)}, v_j^{(\bar{l}_j)}}$ and it queries for a secret key component corresponding to modified hierarchial identity $(I_1^{(l_1)^*}, I_2^{(l_2)^*}, \ldots, I_L^{(l_L)^*})$. Let s be the least identity such that $I_s^{(\bar{l}_s)} \ne I_s^{(l_s)^*}$.
   i. Take $r_1, r_2 \in_R \mathbb{Z}_n$ and implicitly set $\bar{r}_1 = r_1 + \frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}$. Secret key $g, f, v, h_1, \ldots, h_L$ can be obtained by removing the blinding factors $R_g, R_f, R_v, R_{h,1}, \ldots, R_{h,L}$ from $G, F, V, H_1, \ldots, H_L$ respectively.
   ii. Next, $\mathcal{C}$ tries to compute
$$w.\left(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}}\right)^{\bar{r}_1} f^{r_2} = w.\left(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}}\right)^{r_1} f^{r_2}.\left(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}.$$
Using secret keys $v, h_k\ (1 \le k \le s), f$ and public value $I_k^{(l_k)^*}\ (1 \le k \le s)$, $(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}})^{r_1} f^{r_2}$ is computable. Now,
$$w.\left(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}$$
$$= A_{L+1}A_1^\gamma\left(g_p^y.\prod_{k=1}^{L}(A_{L-k+1})^{I_k^{(\bar{l}_k)}} \prod_{k=1}^{s}(g_p^{x_k}/A_{L-k+1})^{I_k^{(l_k)^*}}\right)^{\frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}$$
$$= A_{L+1}A_1^\gamma\left(A_{L+1}^{I_s^{(\bar{l}_s)} - I_s^{(l_s)^*}}.A_s^y.\prod_{k=s+1}^{L}(A_{L+s-k+1})^{I_k^{(\bar{l}_k)}} \prod_{k=1}^{s} A_s^{x_k.I_k^{(l_k)^*}}\right)^{\frac{1}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}$$
$$= A_1^\gamma\left(A_s^y.\prod_{k=s+1}^{L}(A_{L+s-k+1})^{I_k^{(\bar{l}_k)}} \prod_{k=1}^{s} A_s^{x_k.I_k^{(l_k)^*}}\right)^{\frac{1}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}.$$
As $A_k, I_k^{(l_k)^*}, x_k$ values are available, $w.(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}})^{\frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}}$ is computable, so $w.(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}})^{\bar{r}_1}.f^{r_2}$ is also computable.
   iii. Now using Derive algorithm as stated in Algorithm 9, $\mathcal{C}$ computes first component of $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ as $w.(v\prod_{k=1}^{j} h_k^{I_k^{(l_k)^*}})^{\bar{r}_1} f^{r_2}$. Other components $(g^{\bar{r}_1}, g^{r_2}, h_{j+1}^{\bar{r}_1}, \ldots, h_L^{\bar{r}_1})$ of $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ are easily computable using secret key components.

iv. Challenger need to choose $s_1^{(1)}, s_2^{(1)}, s_1^{(2)}, s_2^{(2)} \in_R \mathbb{Z}_n$ such that $s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)} \not\equiv 0 \pmod{q}$, $s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)} \not\equiv 0 \pmod{p}$, for this it check the equation $g_p^{s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)}} \not\equiv 1$ and $g_q^{s_1^{(1)}s_2^{(2)} - s_2^{(1)}s_1^{(2)}} \not\equiv 1$. Components of $sk^{(r)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ are almost same with $sk^{(d)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ except first component does not contain w. So, $\mathcal{C}$ computes $sk^{(r)}_{i,v_i^{(l_i)},v_j^{(l_j)}}$ as previous. Similarly, it can generate secret key $sk_{i,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}$.

v. Adversary gets $sk_i = \{sk_{i,v_i^{(l_i)},v_j^{(l_{j_1})}}, sk_{i,v_i^{(l_i)},v_j^{(l_{j_2})}}, sk_{i,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}\}$, where user i is at $v_L^{(l_L)}$ and $v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})$.

4. Challenge: $\mathcal{A}$ sends two messages $m_0 = (M_0||K), m_1 = (M_1||K)$ to $\mathcal{C}$, where last k bits of each message is K. $\mathcal{C}$ computes ciphertext components following Algorithm 7 as follows. For $1 \le i \le l_0 - h + 1$, C_i's are encryption of m_0 for identity $\mathsf{ID}_{i,0} = (I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_L^{(l_L)})$ and for $l_0 - h + 2 \le i \le l$, C_i's are encryption of m_0 for some random identity $(I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_L^{(l_L)})$ as

$$C_i = \left(m_o.E^s, G^s.Z_1, F^s.Z_2, (V\prod_{k=1}^{L} H_k^{I_k^{(l_k)}})^s.Z_3\right), \quad 1 \le i \le l_0 - h$$

$$C_i = \left(m_0.E^s.T, G^s.Z_1, F^s.Z_2, (V\prod_{k=1}^{L} H_k^{I_k^{(l_k)}})^s.Z_3\right), \quad l_0 - h + 2 \le i \le l$$

$$C_{l_0-h+1} = \left(m_0.T.e(A_1, h^\gamma), h.Z_1, h^z.Z_2, h^{y+\sum_{k=1}^{L} I_k^{(l_k)}.x_k}.Z_3\right),$$

where $Z_1, Z_2, Z_3 \in_R \mathbb{G}_q, s \in_R \mathbb{Z}_n, T \in_R \mathbb{G}_{T,p}$.

$\mathcal{C}$ permutes the C_i values using permutation μ and sends ciphertext $\{k, K, C_{\mu(1)}, \ldots, C_{\mu(l)}\}$ to $\mathcal{A}$. As g_p is generator for $\mathbb{G}_p$, let us consider $h = {g_p}^c$, for some integer c. If $T = e(g_p, {g_p}^c)^{\alpha^{L+1}}$ then ciphertext component

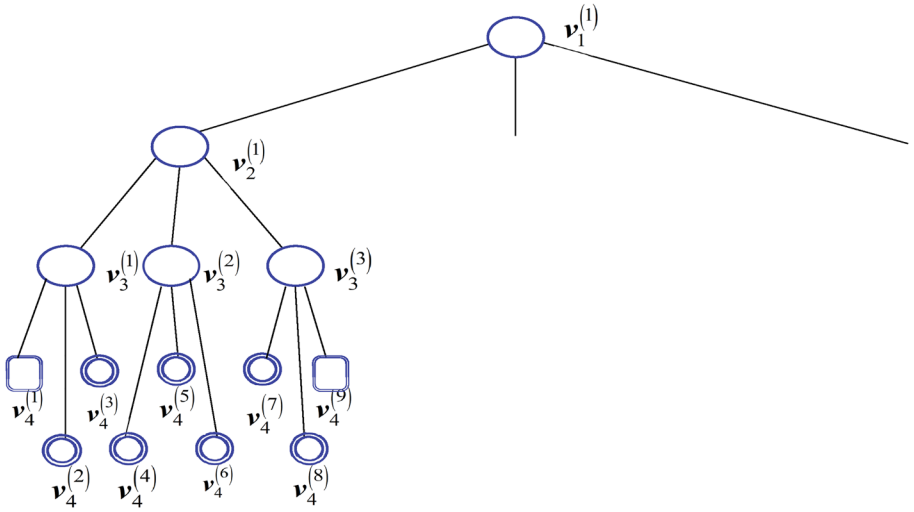

Fig. 5 First 9 nodes in a tree with revoked user at $\{v_4^{(1)}, v_4^{(9)}\}$

Table 3 Encryption, decryption time (in s) and storage (in bytes) for different number of subscribers

No of Subscribers	Encryption time	Increase percentage	Decryption time for PKBE	Increase percentage	Decryption time for OAnoBE	Increase Percentage	PK storage	SK storage per user
9	0.017551	–	0.010111	–	0.030333	–	512	192
27	0.017958	2.324	0.010311	1.97	0.092799	205	576	576
81	0.0180037	0.25	0.010421	1.06	0.281367	203	640	1152
243	0.019943	10.27	0.010496	0.7	1.21176	330	704	1920
729	0.020196	1.26	0.010638	1.35	2.585034	113	768	2880

$$C_{l_0-h+1} = \Big(m_0.e(g_p, {g_p}^c)^{\alpha^{L+1}}.e(A_1, h^\gamma), h.Z_1, h^z.Z_2, h^{\gamma+\Sigma_{k=1}^{L} I_k^{(l_k)}.x_k}.Z_3\Big)$$
$$= \Big(m_0.E^c, G^c.Z_1', F^c.Z_2', (V\prod_{k=1}^{L} H_k^{I_k^{(l_k)}})^c.Z_3'\Big)$$
where $Z_1, Z_2, Z_3 \in \mathbb{G}_q$.

This implies, if $T = e(g_p, {g_p}^c)^{\alpha^{L+1}}$ then ciphertext $\{k, K, C_{\mu(1)}, \ldots, C_{\mu(l)}\}$ is for $\overline{\mathsf{Game}}^0_{h-1}$ else it is for $\overline{\mathsf{Game}}^0_h$.

5. Phase 2: Same as Phase 1.
6. Guess: $\mathcal{A}$ wins the game if he can predict that ciphertext is for $\overline{\mathsf{Game}}^0_{h-1}$ or $\overline{\mathsf{Game}}^0_h$.

Adversary's advantage of distinguishing $\overline{\mathsf{Game}}^0_{h-1}$ and $\overline{\mathsf{Game}}^0_h$ is same as deciding $T = e(g_p, {g_p}^c)^{\alpha^{L+1}}$ or not, i.e., solving L-wDBDHI* problem.

In $\overline{\mathsf{Game}}^0_h$, for $i = l_0 - h + 1$ to l, ciphertext is of the form $(\widehat{C}_1.R_p, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$, where $R_p \in_R \mathbb{G}_{T,p}$. Let R be a random element from $\mathbb{G}_T$. Seo et al. (2009) has proved indistinguishability of $(\widehat{C}_1.R_p, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ from $(\widehat{C}_1.R = R_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ under BSD assumption. Again $(\widehat{C}_1.R = R_1, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ are indistinguishable from (R_1, R_2, R_3, R_4) under L-cDDH assumption (Seo et al. 2009). So, $(\widehat{C}_1.R_p, \widehat{C}_2, \widehat{C}_3, \widehat{C}_4)$ and (R_1, R_2, R_3, R_4) are indistinguishable under L-wDBDHI*, BSD and L-cDDH assumption. This implies that Game^0_{h-1} and Game^0_h are indistinguishable under same assumptions. □

Lemma 4 Game^1_{k-1} *and* Game^1_k *are indistinguishable under L-wDBDHI*, BSD and L-cDDH assumptions.*

The proof of this Lemma is analogous to that of Lemma 3.

•*Special Variant of OAnoBE*

Let $\{v_L^{(l_i)} | 1 \le l_i \le N\}$ be leaf nodes of a tree. We fix $\{v_L^{(l_i)} | l_i = 1, 9i, 9i+1, 1 \le i \le \lfloor N/9 \rfloor\}$ as revoked users for our improved varient. Let $l_i' = \lceil \frac{l_i}{3} \rceil$, $l_i'' = \lceil \frac{l_i}{9} \rceil$. All subsets in cover can be found as follows:

1. If $v_{L-1}^{(l_i')}$ has less than 3 children in ST(R), and head has 3 children, then add $S_{u, v_{L-1}^{(l_i')}, v_L^{(l_{j_1})}}$ or $S_{u, v_{L-1}^{(l_i')}, v_L^{(l_{j_1})} + v_L^{(l_{j_2})}}$ to the cover.
2. If $v_{L-2}^{(l_i'')}$ has 2 children in ST(R), add $S_{u, v_{L-2}^{(l_i'')}, v_{L-1}^{(l_{j_1})} + v_{L-1}^{(l_{j_2})}}$ to the cover.

For each tree with height 3, head node and its ancestor has at least 3 children in ST(R), so cover finding algorithm ensures that on this construction, no height 3 tree will be added into the cover.

The secret keys of user u is $sk_u = \{sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_2})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}} | L-2 \le i \le L-1, i+1 \le j \le L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$. On decryption time user uses these secret keys to decrypt l ciphertext component. So decryption attempt is at most $O(l)$.

Example For Fig. 5, the Cover with respect to revoked users is determined as follows:

(i) The chain C_1 corresponding to the revoked user $v_4^{(1)}$ is $v_3^{(1)}, v_4^{(1)}$, yielding the subset cover $S_{v_3^{(1)}, v_4^{(1)}}$.
(ii) The chain C_2 corresponding to the revoked user $v_4^{(9)}$ is $v_3^{(3)}, v_4^{(9)}$, yielding the subset cover $S_{v_3^{(3)}, v_4^{(9)}}$.
(iii) The head nodes $v_3^{(1)}$ and $v_3^{(3)}$ of the chains C_1, C_2 are then added to R. The nodes $v_4^{(1)}, v_4^{(9)}$ are removed from R and the chain corresponding to $v_3^{(1)}$ (or $v_3^{(3)}$) is $v_2^{(1)}, v_3^{(1)}; v_3^{(3)}$, yielding the set $S_{v_2^{(1)}, v_3^{(1)} + v_3^{(3)}}$.
(iv) Subtree at $v_3^{(1)}, v_3^{(3)}, v_2^{(1)}$, will be added in cover.
(v) Taking $v_1^{(1)}$ as head we can not find any chain, so no new cover will be added.

5 Implementation and evaluation

We have implemented our PKBE in a desktop with the following specification: Dell with Intel(R) Core(TM) i7-7700, 3.60GHz processor, 8GB memory, and Ubuntu 18.04 operating system with the assistance of Pairing-Based Cryptography library (Lynn et al. 2006), version 0.5.12. PBC library is a C library which is built above GNU Math Precision library. We use elliptic curve group on the super singular curve $y^2 = x^3 + x$ and type A1 pairing with composite order group order (consists of 256 bit primes) (see Table 3).

Our OAnoBE has encryption cost similar to PKBE as both encryption are similar except some extra random component which needs negligible time. We have also compared the increase of encryption and decryption cost in percentage (refereed to previous encryption cost). Our OAnoBE has decryption cost more than PKBE as it need to decrypt the ciphertext without knowing the revoked set.

In Table 1, we have given the comparison results with existing similar works. As the constructions are in generic model or in symmetric key setting, therefore we have not implemented their schemes as it would be an unfair comparison.

Future direction The ciphertext size of our constructions can be reduced $\min\{N/k, N-r, 2r-1\}$ using k-ary subset-difference (Bhattacherjee and Sarkar 2015) scheme in a similar manner. However, the decryption cost will be increased. Traitor tracing is a variant of broadcast encryption which helps to trace the leakage of security information by using a tracing algorithm. Another open problem is to extend our OAnoBE construction to a tracing scheme. It would be

more exciting if our construction can be extended to provide full anonymity.

6 Conclusion

We have designed broadcast encryption namely PKBE in public key setting employing *ternary tree subset difference* method. It achieves the revocation property which is one of the most significant requirement in broadcast encryption setting. Our scheme is based on composite order bilinear group and is proven to have selective semantic security in a standard model under reasonable standard assumptions. The extended version of the scheme namely OAnoBE provides outsider-anonymity. Draw back of our construction is that it uses composite order group system. To achieve the security similar to a prime order scheme, it needs to use a composite order group of larger order. We can extend our construction using k-ary SD (Bhattacherjee and Sarkar 2015) scheme in a similar manner as in this work and can further reduce the ciphertext size to $\min\{\frac{N}{k}, N-r, 2r-1\}$. However, the decryption cost will be increased. Moreover, it will be interesting to check whether our schemes provide tracing or not.

Funding Supported by institute post-doctoral fellowship (file no-NISER/R&D/PDF/2019/1484) of National Institute of Science Education and Research Bhubaneswar, HBNI, India.

Appendix

Derive The Derive algorithm works as follows:

Algorithm 9 Derive

input: Secret key $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}} = \left(sk^{(d)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}, sk^{(r)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}\right) = \Big((a_0, a_1, a_2, b_j, b_{j+1}, \ldots, b_L), (\alpha_0^{(x)}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_j^{(x)}, \beta_{j+1}^{(x)}, \ldots, \beta_L^{(x)})_{x=1,2}\Big)$ corresponding to $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})})$, PK,MK, $(I_i^{(l_i)}, \ldots, I_j^{(l_j)})$.

output: Secret key $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$ corresponding to modified hierarchial identity $(I_i^{(l_i)}, \ldots, I_j^{(l_j)})$.

Update secret keys using delegation followed by re-randomization process described below

1. *Delegation procedure:* Compute the followings using $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$:

$$\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = (\zeta_0, \zeta_1, \zeta_2, \eta_{j+1}, \ldots, \eta_L) = \left(a_0 (b_j)^{I_j^{(l_j)}}, a_1, a_2, b_{j+1}, \ldots, b_L\right)$$

$$\widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \left((\theta_0^{(x)}, \theta_1^{(x)}, \theta_2^{(x)}, \phi_{j+1}^{(x)}, \ldots, \phi_L^{(x)})_{x=1,2}\right)$$

$$= \left((\alpha_0^{(x)} (\beta_j^{(x)})^{I_j^{(l_j)}}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_{j+1}^{(x)}, \ldots, \beta_L^{(x)})_{x=1,2}\right).$$

2. Pick random $\gamma_1, \gamma_2, \gamma_3, \delta_1, \delta_2, \delta_3$ from $\mathbb{Z}_n$ satisfying $g_p^{\gamma_2\delta_3 - \gamma_3\delta_2} \not\equiv 1 \pmod{p}$ and $g_q^{\gamma_2\delta_3 - \gamma_3\delta_2} \not\equiv 1 \pmod{q}$.
3. *Re-randomization procedure:* Using $\widetilde{sk}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \left(\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}, \widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}}\right)$, compute $sk_{u,v_i^{(l_i)},v_j^{(l_j)}} = \left(sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}, sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}}\right)$ as follows:

$$sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(\zeta_0(\theta_0^{(1)})^{\gamma_1}(\theta_0^{(2)})^{\delta_1}, \zeta_1(\theta_1^{(1)})^{\gamma_1}(\theta_1^{(2)})^{\delta_1}, \zeta_2(\theta_2^{(1)})^{\gamma_1}(\theta_2^{(2)})^{\delta_1}, \eta_{j+1}(\phi_{j+1}^{(1)})^{\gamma_1}(\phi_{j+1}^{(2)})^{\delta_1}, \ldots, \eta_L(\phi_L^{(1)})^{\gamma_1}(\phi_L^{(2)})^{\delta_1}\Big)$$

$$sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(\Big((\theta_0^{(1)})^{\gamma_x}(\theta_0^{(2)})^{\delta_x}, (\theta_1^{(1)})^{\gamma_x}(\theta_1^{(2)})^{\delta_x}, (\theta_2^{(1)})^{\gamma_x}(\theta_2^{(2)})^{\delta_x}, (\phi_{j+1}^{(1)})^{\gamma_x}(\phi_{j+1}^{(2)})^{\delta_x}, \ldots, (\phi_L^{(1)})^{\gamma_x}(\phi_L^{(2)})^{\delta_x}\Big)_{x=2,3}\Big).$$

Remark $\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}$ can be used to decrypt the ciphertext. Re-randomization is used to re-randomize the secret key obtained in delegation procedure. Note that, the delegation procedure does not need MK and consequently can be run by any entity, who knows the upper level secret key $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$ to derive secret key $\{sk_{u,v_i^{(l_i)},J} | J = v_j^{(l_{j1})}, v_j^{(l_{j2})}, v_j^{(l_{j1})} + v_j^{(l_{j2})}\}$. If we don't use re-randomization procedure then every secret key $\{sk_{u,v_i^{(l_i)},J} | J = v_j^{(l_{j1})}, v_j^{(l_{j2})}, v_j^{(l_{j1})} + v_j^{(l_{j2})}\}$ generated from $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$, will have same randomization exponents r_1, r_2. Dividing first component of $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$ by that of $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j2})}}$, we obtain $\left(h_j^{I_j^{(l_j)}}\right)^{r_1}$. Dividing first component of $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j1})}}$ by $\left(h_j^{I_j^{(l_j)}}\right)^{r_1}$, we can get first component of $sk^{(d)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$. If the hanging nodes are already revoked users and now u revoke, then $sk^{(d)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$ will decrypt the ciphertext (following Decrypt algorithm). Thus a revoked user is still able to recover the message. Re-randomization procedure solves the problem.

Correctness of re-randomization algorithm In Delegation procedure, we generate

$$\begin{aligned}
\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \left(\zeta_0, \zeta_1, \zeta_2, \eta_{j+1}, \eta_{j+2}, \ldots, \eta_L\right)\\
&= \left(a_0 (b_j)^{I_j^{(l_j)}}, a_1, a_2, b_{j+1}, \ldots, b_L\right)\\
&= \left(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{j+1}^{r_1}, \ldots, h_L^{r_1}\right).\\
\widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \left((\theta_0^{(x)}, \theta_1^{(x)}, \theta_2^{(x)}, \phi_{j+1}^{(x)}, \phi_{j+2}^{(x)}, \ldots, \phi_L^{(x)})_{x=1,2}\right)\\
&= \left((\alpha_0^{(x)} (\beta_j^{(x)})^{I_j^{(l_j)}}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_{j+1}^{(x)}, \ldots, \beta_L^{(x)})_{x=1,2}\right)\\
&= \left((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{s_1^{(x)}} f^{s_2^{(x)}}, g^{s_1{}^{(x)}}, g^{s_2{}^{(x)}}, h_{j+1}^{s_1{}^{(x)}}, \ldots, h_L^{s_1{}^{(x)}})_{x=1,2}\right).
\end{aligned}$$

In re-randomization procedure we set,

$$\begin{aligned}
sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big(\zeta_0(\theta_0^{(1)})^{\gamma_1}(\theta_0^{(2)})^{\delta_1}, \zeta_1(\theta_1^{(1)})^{\gamma_1}(\theta_1^{(2)})^{\delta_1}, \zeta_2(\theta_2^{(1)})^{\gamma_1}(\theta_2^{(2)})^{\delta_1},\\
&\quad \eta_{j+1}(\phi_{j+1}^{(1)})^{\gamma_1}(\phi_{j+1}^{(2)})^{\delta_1}, \ldots, \eta_L(\phi_L^{(1)})^{\gamma_1}(\phi_L^{(2)})^{\delta_1}\Big)\\
&= \left(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{\widetilde{r_1}} f^{\widetilde{r_2}}, g^{\widetilde{r_1}}, g^{\widetilde{r_2}}, h_{j+1}^{\widetilde{r_1}}, \ldots, h_L^{\widetilde{r_1}}\right),
\end{aligned}$$

where $\widetilde{r_1} = r_1 + s_1^{(1)}\gamma_1 + s_1^{(2)}\delta_1$ and $\widetilde{r_2} = r_2 + s_2^{(1)}\gamma_1 + s_2^{(2)}\delta_1$.

$$\begin{aligned}
sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big(\big((\theta_0^{(1)})^{\gamma_x}(\theta_0^{(2)})^{\delta_x}, (\theta_1^{(1)})^{\gamma_x}(\theta_1^{(2)})^{\delta_x}, (\theta_2^{(1)})^{\gamma_x}(\theta_2^{(2)})^{\delta_x},\\
&\quad (\phi_{j+1}^{(1)})^{\gamma_x}(\phi_{j+1}^{(2)})^{\delta_x}, \ldots, (\phi_L^{(1)})^{\gamma_x}(\phi_L^{(2)})^{\delta_x}\big)_{x=2,3}\Big).\\
&= \left(\big((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{\widetilde{s_1}^{(x)}} f^{\widetilde{s_2}^{(x)}}, g^{\widetilde{s_1}^{(x)}}, g^{\widetilde{s_2}^{(x)}}, h_{j+1}^{\widetilde{s_1}^{(x)}}, \ldots, h_L^{\widetilde{s_1}^{(x)}}\big)_{x=1,2}\right),
\end{aligned}$$

where $\widetilde{s}_1^{(1)} = s_1^{(1)}\gamma_2 + s_1^{(2)}\delta_2, \widetilde{s}_1^{(2)} = s_1^{(1)}\gamma_3 + s_1^{(2)}\delta_3, \widetilde{s}_2^{(1)} = s_2^{(1)}\gamma_2 + s_2^{(2)}\delta_2, \widetilde{s}_2^{(2)} = s_2^{(1)}\gamma_3 + s_2^{(2)}\delta_3$.

References

AACS (2005) Advanced access content system

Acharya K (2020) Secure and efficient public key multi-channel broadcast encryption schemes. J Inf Secur Appl 51:102436. https://doi.org/10.1016/j.jisa.2019.102436

Acharya K, Dutta R (2016) Secure and efficient construction of broadcast encryption with dealership. Springer International Publishing, Cham, pp 277–295. https://doi.org/10.1007/978-3-319-47422-9_16

Acharya K, Dutta R (2017) Provable secure constructions for broadcast encryption with personalized messages. In: Okamoto T, Yu Y, Au MH, Li Y (eds) Provable security. Springer International Publishing, Cham, pp 329–348

Acharya K, Dutta R (2018a) Constructions of secure multi-channel broadcast encryption schemes in public key framework. In: Camenisch J, Papadimitratos P (eds) Cryptology and network security. Springer International Publishing, Cham, pp 495–515

Acharya K, Dutta R (2018b) Recipient revocable broadcast encryption schemes without random oracles. In: Kim H, Kim DC (eds) Information security and cryptology-ICISC 2017. Springer International Publishing, Cham, pp 191–213

Barth A, Boneh D, Waters B (2006) Privacy in encrypted content distribution using private broadcast encryption. In: Proceedings of the 10th International Conference on financial cryptography and data security, Springer-Verlag, Berlin, Heidelberg, FC'06, pp 52–64, https://doi.org/10.1007/11889663_4

Bhattacherjee S, Sarkar P (2015) Tree based symmetric key broadcast encryption. J Discr Algorithms 34(C):78–107. https://doi.org/10.1016/j.jda.2015.05.010

Boneh D, Hamburg M (2008) Generalized identity based and broadcast encryption schemes. In: Pieprzyk J (ed) Advances in cryptology-ASIACRYPT 2008, vol 5350. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 455–470. https://doi.org/10.1007/978-3-540-89255-7_28

Boneh D, Silverberg A (2003) Applications of multilinear forms to cryptography. Contemp Math 324(1):71–90

Boneh D, Waters B (2006) A fully collusion resistant broadcast, trace, and revoke system. In: Proceedings of the 13th ACM Conference on computer and communications security, ACM, New York, NY, USA, CCS '06, pp 211–220, https://doi.org/10.1145/1180405.1180432

Boneh D, Zhandry M (2014) Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In: Garay J, Gennaro R (eds) Advances in cryptology-CRYPTO 2014, vol 8616. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 480–499. https://doi.org/10.1007/978-3-662-44371-2_27

Boneh D, Gentry C, Waters B (2005) Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Proceedings of the 25th Annual International Conference on advances in cryptology, Springer, Berlin, Heidelberg, CRYPTO'05, pp 258–275. https://doi.org/10.1007/11535218_16

Boneh D, Sahai A, Waters B (2006) Fully collusion resistant traitor tracing with short ciphertexts and private keys. In: Vaudenay S (ed) Advances in cryptology-EUROCRYPT 2006, vol 4004. Lecture notes in computer science. Springer Berlin Heidelberg, Berlin, pp 573–592. https://doi.org/10.1007/11761679_3

Boneh D, Waters B, Zhandry M (2014) Low overhead broadcast encryption from multilinear maps. In: Garay J, Gennaro R (eds) Advances in cryptology-CRYPTO 2014, vol 8616. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 206–223. https://doi.org/10.1007/978-3-662-44371-2_12

Chen L, Li J, Zhang Y (2020) Adaptively secure efficient broadcast encryption with constant-size secret key and ciphertext. Soft Comput 24:4589–4606

Chor B, Fiat A, Naor M (1994) Tracing traitors. In: Proceedings of the 14th Annual International Cryptology Conference on advances in cryptology, Springer-Verlag, London, UK, CRYPTO '94, pp 257–270

Coron JS, Lepoint T, Tibouchi M (2013) Practical multilinear maps over the integers. In: Canetti R, Garay J (eds) Advances in cryptology-CRYPTO 2013, vol 8042. Lecture notes in computer science. Springer Berlin Heidelberg, Berlin, pp 476–493. https://doi.org/10.1007/978-3-642-40041-4_26

Delerablée C (2007) Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Proceedings of the Advances in Crypotology 13th International Conference on theory and application of cryptology and information security, Springer, Berlin, Heidelberg, ASIACRYPT'07, pp 200–215

Delerablée C, Paillier P, Pointcheval D (2007) Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: Takagi T, Okamoto E, Okamoto T, Okamoto T (eds) Pairing, vol 4575. Lecture notes in computer science. Springer, Berlin, pp 39–59

Dodis Y, Fazio N (2003) Public key broadcast encryption for stateless receivers. In: Feigenbaum J (ed) Digital rights management. Springer, Berlin Heidelberg, Berlin, pp 61–80

ElGamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31(4):469–472

Fazio N, Perera I (2012) Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Fischlin M, Buchmann J, Manulis M (eds) Public key cryptography-PKC 2012, vol 7293. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 225–242. https://doi.org/10.1007/978-3-642-30057-8_14

Fiat A, Naor M (1994) broadcast encryption. in: proceedings of the 13th annual international cryptology conference on Advances in Cryptology, Springer-Verlag New York, Inc., New York, NY, USA, CRYPTO '93, pp 480–491

Fukushima K, Kiyomoto S, Tanaka T, Sakurai K (2009) Ternary subset difference method and its quantitative analysis. In: Chung KL, Sohn K, Yung M (eds) Information Security Applications. WISA 2008. Lecture Notes in Computer Science, vol 5379. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-00306-6_17

Garg S, Gentry C, Halevi S (2013a) Candidate multilinear maps from ideal lattices. In: Johansson T, Nguyen P (eds) Advances in cryptology-EUROCRYPT 2013, vol 7881. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 1–17. https://doi.org/10.1007/978-3-642-38348-9_1

Garg S, Gentry C, Halevi S, Raykova M, Sahai A, Waters B (2013b) Candidate indistinguishability obfuscation and functional encryption for all circuits. In: Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on, IEEE, pp 40–49

Ge A, Wei P (2019) Identity-based broadcast encryption with efficient revocation. In: Lin D, Sako K (eds) Public-key cryptography-PKC 2019. Springer International Publishing, Cham, pp 405–435

Gentry C, Waters B (2009) Adaptive security in broadcast encryption systems (with short ciphertexts). In: Joux A (ed) Advances in cryptology-EUROCRYPT 2009, vol 5479. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 171–188. https://doi.org/10.1007/978-3-642-01001-9_10

Gritti C, Susilo W, Plantard T, Liang K, Wong D (2015) Broadcast encryption with dealership. Int J Inf Secur. https://doi.org/10.1007/s10207-015-0285-x

Halevy D, Shamir A (2002) The lsd broadcast encryption scheme. In: Yung M (ed) Advances in cryptology-CRYPTO 2002, vol 2442. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 47–60. https://doi.org/10.1007/3-540-45708-9_4

Hu C, Liu P, Guo S (2016) Public key encryption secure against related-key attacks and key-leakage attacks from extractable hash proofs. J Ambient Intell Hum Comput 7(5):681–692

Ke L, Yi Z, Ren Y (2015) Improved broadcast encryption schemes with enhanced security. J Ambient Intell Hum Comput 6(1):121–129

Lai J, Mu Y, Guo F, Susilo W, Chen R (2016) Anonymous identity-based broadcast encryption with revocation for file sharing. In: Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II, pp 223–239, https://doi.org/10.1007/978-3-319-40367-0_14

Lai J, Mu Y, Guo F, Chen R (2017) Fully privacy-preserving id-based broadcast encryption with authorization. Comput J 60(12):1809–1821. https://doi.org/10.1093/comjnl/bxx060

Lewko A, Sahai A, Waters B (2010) Revocation systems with very small private keys. In: Security and Privacy (SP), 2010 IEEE Symposium on, pp 273–285, https://doi.org/10.1109/SP.2010.23

Li J, Chen L, Lu Y, Zhang Y (2018a) Anonymous certificate-based broadcast encryption with constant decryption cost. Inf Sci 454–455:110–127

Li J, Yu Q, Zhang Y (2018b) Identity-based broadcast encryption with continuous leakage resilience. Inf Sci 429(C):177–193

Libert B, Paterson K, Quaglia E (2012) Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model. In: Fischlin M, Buchmann J, Manulis M (eds) Public key cryptography-PKC 2012, vol 7293. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 206–224. https://doi.org/10.1007/978-3-642-30057-8_13

Liu J, Ke L (2019) New efficient identity based encryption without pairings. J Ambient Intell Hum Comput 10(4):1561–1570

Liu W, Liu J, Wu Q, Qin B (2014) Hierarchical identity-based broadcast encryption. In: Susilo W, Mu Y (eds) Information security and privacy, vol 8544. Lecture notes in computer science. Springer, Cham, pp 242–257. https://doi.org/10.1007/978-3-319-08344-5_16

Liu W, Liu J, Wu Q, Qin B, Li Y (2015) Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption. Int J Inf Secur. https://doi.org/10.1007/s10207-015-0287-8

Lynn B, et al. (2006) The pairing-based cryptography library. Internet: crypto stanford edu/pbc/[Mar 27, 2013]

Naor D, Naor M, Lotspiech J (2001) Revocation and tracing schemes for stateless receivers. In: Kilian J (ed) Advances in cryptology-CRYPTO 2001, vol 2139. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 41–62. https://doi.org/10.1007/3-540-44647-8_3

Ohtake G, Hanaoka G, Ogawa K (2010) Efficient broadcast encryption with personalized messages. In: Heng SH, Kurosawa K (eds) Provable security. Springer, Berlin Heidelberg, Berlin, pp 214–228

Phan DH, Pointcheval D, Shahandashti S, Strefler M (2013a) Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts. Int J Inf Secur 12(4):251–265. https://doi.org/10.1007/s10207-013-0190-0

Phan DH, Pointcheval D, Trinh VC (2013b) Multi-channel broadcast encryption. In: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ACM, New York, NY, USA, ASIA CCS '13, pp 277–286, https://doi.org/10.1145/2484313.2484348

Ren Y, Niu Z, Zhang X (2014) Fully anonymous identity-based broadcast encryption without random oracles. IJ Netw Secur 16(4):256–264

Sakai R, Furukawa J (2007) Identity-based broadcast encryption. IACR Cryptol ePrint Arch 2007:217

Seo JH, Kobayashi T, Ohkubo M, Suzuki K (2009) Anonymous hierarchical identity-based encryption with constant size ciphertexts. Springer Berlin Heidelberg, Berlin, pp 215–234. https://doi.org/10.1007/978-3-642-00468-1_13

Shamir A (1985) Identity-based cryptosystems and signature schemes. In: Blakley G, Chaum D (eds) Advances in cryptology, vol 196. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 47–53. https://doi.org/10.1007/3-540-39568-7_5

Susilo W, Chen R, Guo F, Yang G, Mu Y, Chow YW (2016) Recipient revocable identity-based broadcast encryption: How to revoke some recipients in ibbe without knowledge of the plaintext. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ACM, New York, NY, USA, ASIA CCS '16, pp 201–210, https://doi.org/10.1145/2897845.2897848

Wu Q, Qin B, Zhang L, Domingo-Ferrer J (2011) Fully distributed broadcast encryption. In: Boyen X, Chen X (eds) Provable security, vol 6980. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 102–119. https://doi.org/10.1007/978-3-642-24316-5_9

Xu K, Liao YL, Qiao Liu Z, Yang X (2015) An identity-based (idb) broadcast encryption scheme with personalized messages (bepm). PLoS One 10(12):e0143975. https://doi.org/10.1371/journalpone0143975

Xu Y, Wu S, Wang M, Zou Y (2020) Design and implementation of distributed rsa algorithm based on hadoop. J Ambient Intell Hum Comput 11(3):1047–1053

Zhao XW, Li H (2013) Improvement on a multi-channel broadcast encryption scheme. Mechanical engineering, Industrial Electronics and Information Technology Applications in Industry, Trans Tech Publications Ltd. Appl Mech Mater 427:2163–2169. https://doi.org/10.4028/www.scientific.net/AMM.427-429.2163