Enhanced Outsider-anonymous Broadcast Encryption with Subset Difference Revocation

Kamalesh Acharya, Ratna Dutta

Department of Mathematics

Indian Institute of Technology Kharagpur, India

kamaleshiitkgp@gmail.com, ratna@maths.iitkgp.ernet.in

Abstract

This paper puts forward an efficient broadcast encryption in public key setting employing *ternary tree subset difference* method for revocation. It provides *outsider anonymity* disabling the revoked users from getting any information of message and *concealing* the set of subscribed users from the revoked users. Our approach utilizes composite order bilinear group setting and exhibits significant improvement in the *broadcast efficiency*. The proposed scheme compares favourably over the existing similar schemes in standard model. The public key and secret key sizes are *poly-logarithmic* while the ciphertext size is *sublinear* in total number of users. Our scheme achieves selective security against chosen plaintext attack in the standard model under reasonable assumptions.

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 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 (Fiat and Naor, 1994) in 1994, followed by subsequent works in various flavours- revocation scheme (DF; Boneh et al., 2005; Halevy and Shamir, 2002; Lewko et al., 2010), identity based scheme (Delerablée, 2007; Sakai and Furukawa, 2007), bilinear map based scheme (Boneh et al., 2005; Gentry, 2006; Phan et al., 2013), multilinear map based scheme (Boneh et al., 2014). It has wide applications in TV and radio subscription services where broadcast messages are encrypted for currently active subscribers.

Basic security property of public key encryption is data secrecy, whereby no information about the original message get 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. The main focus of most of the broadcast encryption schemes referred above is to provide constructions with short parameters in terms of ciphertext overhead, secret key size and public key size. They 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. Barth et al. (Barth et al., 2006) introduced an *anonymous broadcast encryption* scheme to address the privacy issue in broadcast encryption.

Outsider anonymous broadcast encryption is another interesting variant of broadcast encryption that achieves security and privacy of the receivers. Consider following applications:

- 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.

- Soldiers want to send a encrypted message in the air so that enemies cannot extract the original message and the identities of the intended recipients. If enemies can understand who are the opponents, they can compromise with some of the opponents and get important information.

- Suppose prime minister want to discuss some sensitive topic with all chief ministers in an urgent basis. They do not want to reveal the topic and identities of the participants outside the group.

In the aforementioned 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 et al. (Fazio and Perera, 2012).

Our contribution: Protecting user's privacy is the most significant requirement in the context of broadcast encryption apart from user revocation. There is a vast literature on broadcast encryption which does not exibit anonimity inherently. Our goal is to devise new technique for managing revocation while featuring compact ciphertexts, secret keys and public keys with strong security properties.

We summarize below the main findings of this work:

(i) Fazio et al. has devided set of subscribed users in subgroups using binary complete subtree (CS) method. Then gives secret key corresponding to all nodes lies in path joining user u to root. In time of decryption each subscribed user tries to decrypt the ciphertext components by its available secret keys. As user will lie in at least one of complete subtree rooted at one of the node lies in path joining user u to root, user will able to decrypt the ciphertext. The scheme is secure under q-Augmented Decisional Bilinear Diffie-Hellman Exponent (q-ADBDHE) and unforgeability of underline signature scheme.

We propose an *outsider anonymous broadcast encryption* scheme by employing ternary tree subset difference method of Fukushima et al. (Fukushima et al., 2009) to partition subscribed users into groups. For each groups, broadcaster generates ciphertext using anonymous hierarchical identity based encryption of Seo et al. (Seo et al., 2009). Binary *complete subtree* (CS) method of Naor et al. (Naor et al., 2001), partitions subscribed users into $O(r \log_2 \frac{N}{r})$ subsets, while binary subset difference (SD) method (Naor et al., 2001) partitions subscribed users into $O(r)$ subsets. Integrating the *ternary SD revocation method*, we reduce the size of partition, and consequently the ciphertext size, leading to a significant improvement in the broadcast efficiency over existing similar works. A comparative summary of anonymous broadcast encryption schemes are outlined in Table 1. To the best of our knowledge, the major works addressing the issue of anonimity in broadcast encryption appears in (Barth et al., 2006; Fazio and Perera, 2012; He et al., 2016; Libert et al., 2012; Ren et al., 2014; Zhang and Takagi, 2013). The construction of (Fazio and Perera, 2012) provides *outsider anonymity.* They have proposed a scheme using *binary CS* method with public key size $O(N)$, secret key size $O(\log_2 N)$, ciphertext size $O(r \log_2 \frac{N}{r})$, where N and r stands for the total number of users and the number of revoked users respectively. The ciphertext size can be reduced to $\mathsf{min}\{\frac{N}{2}, 2r-1\}$ using binary SD method at the expense of public key and secret key size $O(N \log_2 N)$, $O(N)$ respectively. The description of their SD-based construction is rather informal and detail security proof is not provided. Our scheme enhances the work by Fazio et. al (Fazio and Perera, 2012) in the sense that it reduces the ciphertext size as well as public key size. It reduces the ciphertext size to $\mathsf{min}\{\frac{N}{3}, N-r, 2r-1\}$ using *ternary SD* method at the expense of public key and secret key size $O(\log_3 N)$, $O(\log{}_3{}^2 N)$ respectively. Let L be the level of leaf nodes in a ternary tree. Our scheme is secure under L-weak Decisional Bilinear Deffie-Hellman Inversion assumption, Bilinear Subset Decision assumption and L-composite Decisional Deffie-Hellman assumption. We have proposed an special variant which has constant secret key per each subscribed user and decryption attempt reduces to $O(l)$, where l is theoretical bound of cover size. Zhang et al. (Zhang and Takagi, 2013) has proposed a scheme with ciphertext size $O(N-r)$ but it is in random oracle model. A proof in in the random oracle model can serve only as a heuristic argument, as all parties gets a black box access to a truly random function.

(ii) 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 is issued the set of secret keys in such a way that he will capable to recover the message. None of the existing anonymous constructions discuss revocation process.

(iii) Furthermore, new users can join any time without any updation of 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.

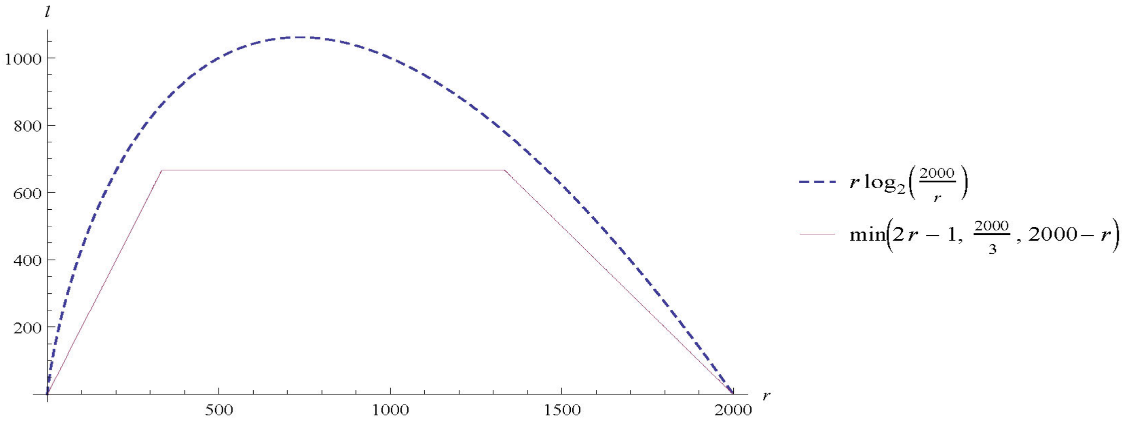

Figure 1: Comparison of cover size (l) against revoked user (r), taking number of user N as 2000.

(iv) Our scheme achieves selective semantic security in standard model under L-weak Decisional Bilinear Deffie-Hellman Inversion assumption, Bilinear Subset Decision assumption and L-composite Decisional Deffie-Hellman assumption. Our proposed scheme can be extended using the k-ary tree (Bhattacherjee and Sarkar, 2015) to provide ciphertext size as $\mathsf{min}\{\frac{N}{k}, N-r, 2r-1\}$ at the cost of decryption time.

Organization: The rest of the paper is organized as follows. We discuss related works in section 2. Section 3 provides necessary definitions and background materials. We describe our main construction in section 4 and prove its security in section 5. Section 6 provides an special variant. We finally conclude in section 7.

Table 1: Comparison of various broadcast encryption schemes.

Scheme	PK size	SK size	CT size	Anon	SM	MC	RO	No-of-dec
Barth et al. (2006)	$O(N)$	$O(1)$	$O(N-r)$	Full	Selective	IND-CCA	No	$O(N-r)$+1
Libert et al. (2012)	$O(N)$	$O(1)$	$O(N-r)$	Full	Adaptive	IND-CCA	No	$O(l)$+1
Ren et al. (2014)	$N+2$	$O(N-r)$	$O(N-r)$	Full	Adaptive	IND-CCA	No	$O(N-r)$
He et al. (2016)	5	1	$N-r+3$	Full	Adaptive	IND-CPA	**Yes**	$O(1)$
Fazio and Perera (2012)	$N+2$	$\log_2 N+1$	$r\log_2\frac{N}{r}$	Outsider	Adaptive	IND-CCA	No	$O(r\log_2 N)$+1
Zhang and Takagi (2013)	2	1	$N-r+3$	Outsider	Adaptive	IND-CCA	**Yes**	$O(N-r)$
Our Scheme	$\log_3 N+6$	$O(\log_3{}^2 N)$	$\mathsf{min}\{\frac{N}{3}, N-r, 2r-1\}$	Outsider	Selective	IND-CPA	No	$O(Nl)$
Our SpeV	$\log_3 N+6$	9	$\mathsf{min}\{\frac{N}{3}, N-r, 2r-1\}$	Outsider	Selective	IND-CPA	No	$O(l)$

PK=public key, SK= secret key, CT=ciphertext, Anon=anonimity, '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. Number of decryption $O(x)+1$ means that it needs $O(x)$ decryption attempt to find the ciphertext decryptable by user and 1 decryption attempt to decrypt the ciphertext, SpeV = special variant

2 Related Works

The concept of broadcast encryption was proposed by Fiat and Naor (Fiat and Naor, 1994) in 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.

1. **Revocation Scheme:** Revocation schemes are broadcast encryption schemes where set of revoked users are taken as input in encryption function. In Crypto 2001, Naor et al. (Naor et al., 2001) suggested two private key broadcast encryption schemes. One of these scheme has ciphertext size $O(r \log_2 \frac{N}{r})$ and key storage $O(\log_2 N)$ per each subscribed user. The other scheme has ciphertext size $O(r)$ and key size $O(\log_2^2(N))$ per each subscribed user. 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 (Halevy and Shamir, 2002) in Crypto 2002. It has public key size $O(\log_2^{1+\epsilon} N)$ and secret key size $O(\frac{r}{\epsilon})$ where $\epsilon > 0$. Dodis and Fazio (DF) converted above schemes in public key setting. In Pairing 2007, Delerablee et al. (Delerablée et al., 2007) proposed a scheme which achieves constant size secret key with ciphertext size $O(r)$ and public key size linear to the number of users. The scheme is indistinguishable under chosen plaintext attack (IND-CPA) in selective security model on the General Decisional Diffie-Helman Exponent (GDDHE) assumption. A broadcast encryption with constant size public key and secret key was proposed by Lewko et al. (Lewko et al., 2010) in Security and Privacy (SP), 2010 IEEE Symposium, where ciphertext size is $O(r)$. It achieves selective IND-CPA security under the q-Multi-Exponent Bilinear Diffie-Hellman (q-MEBDH) assumption.

2. **Algabric Construction using Bilinear and Multilinear map:** The schemes proposed in (DF; Delerablée et al., 2007; Halevy and Shamir, 2002; Lewko et al., 2010; Naor et al., 2001) are efficient to use if $r << N$. On the other hand, if $N - r << N$, i.e., if the revoked set is very large and the subscribed set is very less, then these schemes are not efficient as the computation cost will be increased. We will discuss some algabric construction using bilinear and multilinear map. In Crypto 2005, Boneh et al. (Boneh et al., 2005) presented a semantically secure broadcast encryption scheme with constant ciphertext, secret key size while public key size is $O(N)$. Above broadcast encryption system is semantically secure if the N-Decisional Bilinear Diffie-Hellman Exponent (N-DBDHE) assumption holds. A semi-static secure broadcast encryption was proposed by Gentry et al. (Gentry, 2006) in Eurocrypt 2009, where the public key, secret key, ciphertext sizes are $O(N)$, $O(N)$, $O(1)$ respectively. Furthermore, they converted it into adaptive secure model. In IJIS 2013, Phan et al. (Phan et al., 2013) developed a scheme with public key size $O(N)$, secret key size $O(1)$, ciphertext size $O(1)$ and achieves selective IND-CCA security under N-DBDHE assumption. In Crypto 2014, Boneh et al. (Boneh et al., 2014) presented a scheme using multilinear map (Boneh and Silverberg, 2003; Coron et al., 2013; Garg et al., 2013a,0), with constant ciphertext and secret key size, whereas public key size is $O(\log_2 N)$. The scheme is selective IND-CPA secure under N-Hybrid Diffie-Hellman Exponent (N-HDHE) assumption.

3. **Identity Based Scheme:** Identity based encryption scheme was introduced by Shamir (Shamir, 1985). Delerablée (Delerablée, 2007) proposed first identity based broadcast encryption scheme in Pairing 2007. The scheme achieves constant ciphertext and secret key size and indistinguishable under chosen plaintext attack in selective ID model under the GDDHE assumption. Sakai et al. (Sakai and Furukawa, 2007) came up with a identity based broadcast encryption scheme on additive bilinear group with constant private key and ciphertext size. In Asiacrypt 2008, Boneh et al. (Boneh and Hamburg, 2008) proposed generalised identity based encryption scheme with public key size $O(N)$, private key size $O(1)$, ciphertext size $O(1)$ respectively. The scheme is key indistinguishable under adaptive key exchange attack in generic bilinear group model with random oracle.

4. **Traitor Tracing Scheme:** An important property on broadcast encryption scheme is the traceability. Traitor tracing scheme was introduced by Chor et al. (Chor et al., 1994) on Crypto 1994. Boneh, Sahai, Waters (Boneh et al., 2006) proposed first collision resistance scheme using private linear broadcast encryption. It has public key size $O(\sqrt{N})$, private key size $O(1)$, ciphertext size $O(\sqrt{N})$ respectively. The scheme is secure in index hiding game under decisional 3 party Diffie-Hellman, bilinear subgroup decision, subgroup decision assumption. Trace and revoke scheme is a combination of broadcast encryption and tracing scheme. Boneh and Waters (Boneh and Waters, 2006) proposed a scheme with all the above parameters as $O(\sqrt{N})$. The scheme is secure in index hiding game under decisional 3 party Diffie-Hellman assumption. Boneh et al. (Boneh and Zhandry, 2014) proposed a scheme using indistinguishability obfuscation where key size linear to logarithm of N. Security of this scheme lies on security of underlying pseudo random function.

5. **Distributed Broadcast Encryption Scheme:** In ProvSec 2014, Wu et al. (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. The scheme obtains public key size $O(N)$, private key size $O(1)$, ciphertext size $O(1)$ respectively. Boneh et al. (Boneh and Zhandry, 2014) proposed a scheme using indistinguishability obfuscation in Crypto 2014. It has public key size $O(N)$, private key size $O(1)$, ciphertext size $O(1)$ and achieves IND-CCA security under the existance of multiparty key exchange protocol.

6. **Hierarchial Broadcast Encryption Scheme:** In ACISP 2014, Liu et al. (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. The scheme obtain public key size $O(N)$, private key size $O(N)$, ciphertext size constant. They proposed a CCA secure version (Liu et al., 2015) in IJIS 2015.

7. **Broadcast Encryption with Dealership Scheme:** Gritti et al. (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 and have public key size $O(N)$, private key size $O(1)$, ciphertext size $O(1)$ respectively. In this construction broadcaster need to rely on user response to detect a dishonest dealer. Acharya et al. (Acharya and Dutta, 2016) has solved the problem and proposed a scheme with constant communication.

8. **Anonymous Scheme:** In FCDS 2006, Barth et al. (Barth et al., 2006) proposed a new variant of broadcast encryption, called as *private broadcast encryption* or *anonymous broadcast encryption* (AnoBE) with public key size $O(N)$, secret key size $O(1)$, ciphertext size $O(N-r)$. The scheme is selective IND-CCA secure in random oracle model. An adaptive IND-CCA secure scheme with same parameters and standard security model was developed by Libert et al. (Libert et al., 2012) in PKC 2012. In IJNS 2014, Ren et al. (Ren et al., 2014) came up with the first identity based *anonymous broadcast encryption* scheme with public key size $O(N)$, secret key size $O(N-r)$ and ciphertext size $O(N-r)$. The scheme is adaptive IND-CPA secure under asymmetric decisional Bilinear Diffie-Hellman assumption. Fazio et al. (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.

3 Preliminaries

3.1 Outsider-anonymous Broadcast Encryption

An *outsider-anonymous broadcast encryption* scheme OAnoBE= (Setup, $\mathsf{KeyGeneration}$, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$) consists of 3 probabilistic polynomial time algorithms Setup, $\mathsf{KeyGeneration}$, $\mathsf{Encrypt}$ and 1 deterministic polynomial time algorithm $\mathsf{Decrypt}$.

$\mathsf{Setup}(N, \lambda)$: 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.

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

$\mathsf{Encrypt}(\mathbb{R}, \mathsf{PK}, m)$: 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.

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

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.

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., $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{KeyGeneration}(\mathsf{PK}, \mathsf{MK}, i), \mathsf{Encrypt}(\mathbb{R}, \mathsf{PK}, m))$ $= m$, for every revoked set $\mathbb{R}$, every message m.

3.2 Security Game

We define below *selective semantic security* of our revocation scheme OAnoBE= (Setup, $\mathsf{KeyGeneration}$, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$) following outsider anonymous scheme of Fazio et al. (Fazio and Perera, 2012) and revocation scheme of Naor et al. (Naor et al., 2001) 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: The challenger $\mathcal{C}$ runs $(\mathsf{PK}, \mathsf{MK}) \leftarrow \mathsf{Setup}(N, \lambda)$. It keeps MK secret to itself and makes PK public.

Phase 1: The adversary $\mathcal{A}$ sends key generation query for $i_1, \ldots, i_m \in \mathbb{R}_0 \cap \mathbb{R}_1$ 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

$$Adv_{\mathcal{A}}^{\mathsf{OAnoBE\text{-}IND\text{-}CPA}} = |Pr(b' = b) - \frac{1}{2}|.$$

The probability is over random bits used by $\mathcal{C}$ and $\mathcal{A}$.

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

3.3 Complexity Assumptions

Definition 2. *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 $\mathbb{N}, \mathbb{R}$ are sets of natural and real numbers respectively. Let $\epsilon : \mathbb{N} \to \mathbb{R}$ be a function. If $\exists$ $d \in \mathbb{N}$ 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 adversary $\mathcal{A}$ 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 $T \in \mathbb{G}_{T,p}$, $T^* \in \mathbb{G}_T$.
  BSD Assumption: For any PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{BSD}$ is negligible.

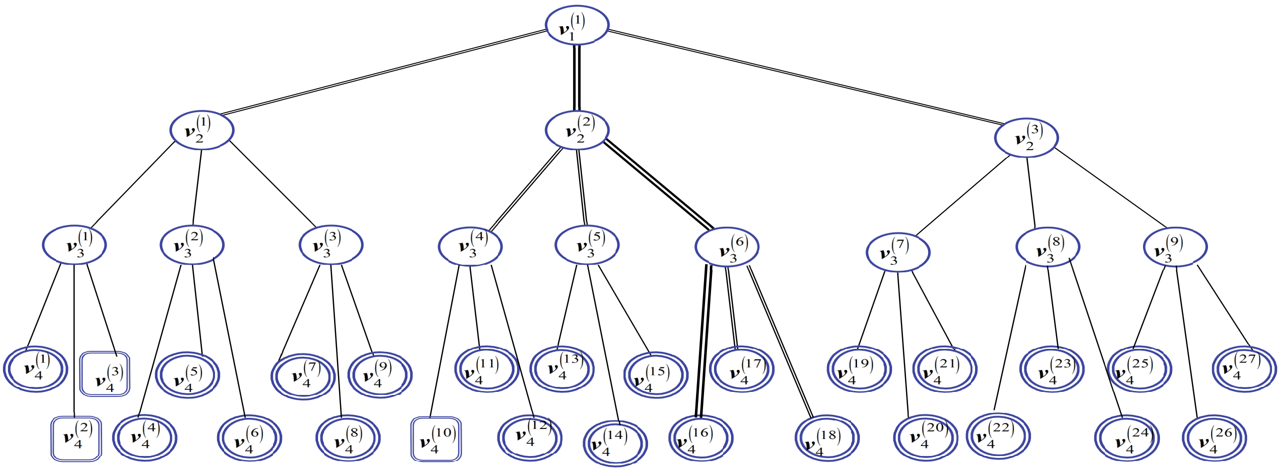

Figure 2: Labeling of nodes of a complete ternary tree with revoked users $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$, where double-thick lines represent a path from the root node $v_1^{(1)}$ to the user u at $v_4^{(16)}$, double-thin lines denote the edges just hanging off this path, circular nodes represent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

3.4 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 power of 3. We level the nodes as in Figure 1. 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, $\mathsf{ST}(R)$ 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

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

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 3. *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* $\mathsf{ST}(R)$*:*

(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.*

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
```

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 $S_{v_i^{(l_i)},v_j^{(l_j)}}$ 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 $1 \leq i \leq \log_3 N+1, 1 \leq l_i \leq 3^{i-1}$. 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 4. *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 $\mathsf{ID}|_{v_j^{(l_j)}}$.*

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 $\mathsf{ST}(R)$ 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 $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$, $\ldots$, $v_j^{(l_{j1})}; v_j^{(l_{j2})}$.
       (b) Add $S_{v_i^{(l_i)},J}$ ($J = v_j^{(l_j)}$ or $v_j^{(l_{j1})} + v_j^{(l_{j2})}$) to the Cover and add $v_i^{(l_i)}$ to $R$ and remove
           $v_j^{(l_j)}$ or $v_j^{(l_{j1})}; v_j^{(l_{j2})}$ 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 $v_i^{(l_i)}$, $v_{i+1}^{(l_{i+1})}$,$\ldots$, $v_j^{(l_{j1})}; v_j^{(l_{j2})}$, $\mathsf{parent}(v_i^{(l_i)})$ is either the root node or a node with 2 or 3 children in $\mathsf{ST}(R)$. 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 $\mathsf{ST}(R)$, 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 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 1, $\mathsf{PN}(v_4^{(16)}) = \{v_1^{(1)}, v_2^{(2)}, v_3^{(6)}, v_4^{(16)}\}$ 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 Figure 2. The Cover with respect to R is determined as follows:

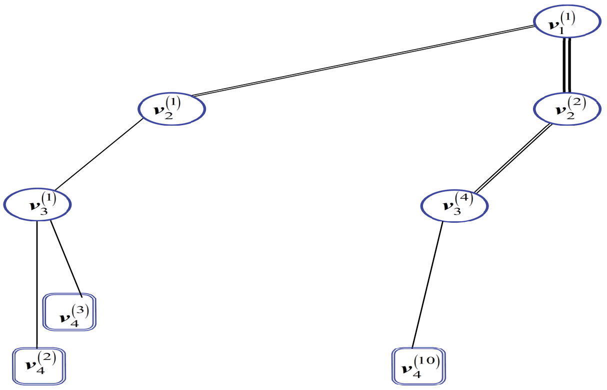

Figure 3: Steiner Tree $\mathsf{ST}(R)$ for Figure 1 where $R = \{v_4^{(2)}, v_4^{(3)}, v_4^{(10)}\}$

(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

$$\begin{aligned} S_{v_2^{(1)}, v_4^{(2)}+v_4^{(3)}} &= \{v_4^{(1)}, v_4^{(4)}, v_4^{(5)}, v_4^{(6)}, v_4^{(7)}, v_4^{(8)}, v_4^{(9)}\}, \\ S_{v_2^{(2)}, v_4^{(10)}} &= \{v_4^{(11)}, v_4^{(12)}, v_4^{(13)}, v_4^{(14)}, v_4^{(15)}, v_4^{(16)}, v_4^{(17)}, v_4^{(18)}\}, \\ S_{v_1^{(1)}, v_2^{(1)}+v_2^{(2)}} &= \{v_4^{(19)}, v_4^{(20)}, v_4^{(21)}, v_4^{(22)}, v_4^{(23)}, v_4^{(24)}, v_4^{(25)}, v_4^{(26)}, v_4^{(27)}\}. \end{aligned}$$

4 Our Scheme

Our *outsider-anonymous broadcast encryption* scheme OAnoBE= (Setup, KeyGeneration, Encrypt, Decrypt) couples the anonymous hierarchical encryption scheme of Seo et al. (Seo et al., 2009) and ternary tree SD revocation of Fukushima et al. (Fukushima et al., 2009).

Our scheme 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 below in algorithm 3-7.

The PKGC generates the public and the master key using Setup algorithm. It keeps the master key private to itself and publishes the public key. The subscribed user at a leaf node gets 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 helps to compute secret key of children using 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. To preserve the anonymity, the broadcaster also generates $(l - |Cover|)$ many dummy ciphertext components, where l is theoretical bound of cover size. The subscribed user u attempts to decrypt the ciphertext components using the secret keys received from the PKGC in KeyGeneration phase and utilizing the delegation mechanism of algorithm Derive. It succeeds in recovering the message either by the secret key corresponding to hanging nodes else by the derived keys.

```
Algorithm 3 Setup
input: Security parameter $\lambda$, 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 $\lambda$. 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 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 $v_L^{(l_L)}$. For the user u at leaf $v_L^{(l_L)}$, $v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)})$ at level i, $v_j^{(l_j)} \in \mathsf{PN}(v_L^{(l_L)}) \cup \mathsf{HN}(v_L^{(l_L)})$ at level j. 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 $sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$ 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$\rangle$ 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$\rangle$ to generate the combined secret key $sk_{u,v_1^{(1)},v_2^{(l_{j1})}+v_2^{(l_{j2})}}$, where $v_2^{(l_{j_1})}, v_2^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})$. 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 $sk_{u,v_1^{(1)},v_3^{(l_{j_1})}+v_3^{(l_{j_2})}}$, where $v_3^{(l_{j_1})}, v_3^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})$. 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 $sk_u = \{sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_2})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}} | 1 \leq i \leq L-1, i+1 \leq j \leq L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$. As an example, in Figure 1, 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: $(I_1^{(l_1)},\ldots,I_L^{(l_L)})$, PK=$(g_p, g_q, G, F, V, H_1, H_2, \ldots, H_L, E, N, \mathbb{S})$, 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
                  $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{j+1}^{r_1}, \ldots, h_L^{r_1}\Big)$
                  $sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{s_1^{(x)}} f^{s_2^{(x)}}, g^{s_1^{(x)}}, g^{s_2^{(x)}}, h_{j+1}^{s_1^{(x)}}, \ldots, h_L^{s_1^{(x)}})_{x=1,2}\Big).$
              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 $j \ne i+1$ 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 5.
           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.

Algorithm 5 Derive

input: Secret key $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}} = \Big(sk^{(d)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}},\ sk^{(r)}_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}\Big){=}\Big((a_0, a_1, a_2,\ b_j, b_{j+1}, \ldots, b_L),$ $(\alpha_0^{(x)}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_j^{(x)}, \beta_{j+1}^{(x)}, \ldots,\ \ \beta_L^{(x)})_{x=1,2}\Big)$ 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 $sk_{u,v_i^{(l_i)},v_{j-1}^{(l_{j-1})}}$:

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

$$\begin{aligned}\widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big((\theta_0^{(x)}, \theta_1^{(x)}, \theta_2^{(x)}, \phi_{j+1}^{(x)}, \ldots, \phi_L^{(x)})_{x=1,2}\Big)\\ &= \Big((\alpha_0^{(x)}(\beta_j^{(x)})^{I_j^{(l_j)}}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_{j+1}^{(x)}, \ldots, \beta_L^{(x)})_{x=1,2}\Big).\end{aligned}$$

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 $\widetilde{sk}_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}},\ \widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}}\Big)$, compute $sk_{u,v_i^{(l_i)},v_j^{(l_j)}} = \Big(sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}},\ sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}}\Big)$ as follows:

$$\begin{aligned}sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big(\zeta_0(\theta_0^{(1)})^{\gamma_1}(\theta_0^{(2)})^{\delta_1}, \zeta_1(\theta_1^{(1)})^{\gamma_1}(\theta_1^{(2)})^{\delta_1}, \zeta_2(\theta_2^{(1)})^{\gamma_1}(\theta_2^{(2)})^{\delta_1},\\ &\quad \eta_{j+1}(\phi_{j+1}^{(1)})^{\gamma_1}(\phi_{j+1}^{(2)})^{\delta_1}, \ldots, \eta_L(\phi_L^{(1)})^{\gamma_1}(\phi_L^{(2)})^{\delta_1}\Big)\\ sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big(\Big((\theta_0^{(1)})^{\gamma_x}(\theta_0^{(2)})^{\delta_x}, (\theta_1^{(1)})^{\gamma_x}(\theta_1^{(2)})^{\delta_x}, (\theta_2^{(1)})^{\gamma_x}(\theta_2^{(2)})^{\delta_x},\\ &\quad (\phi_{j+1}^{(1)})^{\gamma_x}(\phi_{j+1}^{(2)})^{\delta_x}, \ldots, (\phi_L^{(1)})^{\gamma_x}(\phi_L^{(2)})^{\delta_x}\Big)_{x=2,3}\Big).\end{aligned}$$

Remark 1. $\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}}$ *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* $\{sk_{u,v_i^{(l_i)},J} | J = v_j^{(l_{j_1})}, v_j^{(l_{j_2})}, v_j^{(l_{j_1})}+v_j^{(l_{j_2})}\}$. *If we don't use re-randomization procedure then every secret key* $\{sk_{u,v_i^{(l_i)},J} | J = v_j^{(l_{j_1})}, v_j^{(l_{j_2})}, v_j^{(l_{j_1})}+v_j^{(l_{j_2})}\}$ *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* $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}}$ *by that of* $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j_2})}}$, *we obtain* $\left(h_j^{I_j^{(l_j)}}\right)^{r_1}$. *Dividing first component of* $sk^{(d)}_{u,v_i^{(l_i)},v_j^{(l_{j_1})}}$ *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

$$
\begin{aligned}
\widetilde{sk}^{(d)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= (\zeta_0, \zeta_1, \zeta_2, \eta_{j+1}, \eta_{j+2}, \ldots, \eta_L) = \Big(a_0(b_j)^{I_j^{(l_j)}}, a_1, a_2, b_{j+1}, \ldots, b_L\Big) \\
&= \Big(w.(v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{j+1}^{r_1}, \ldots, h_L^{r_1}\Big).
\end{aligned}
$$

$$
\begin{aligned}
\widetilde{sk}^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big((\theta_0^{(x)}, \theta_1^{(x)}, \theta_2^{(x)}, \phi_{j+1}^{(x)}, \phi_{j+2}^{(x)}, \ldots, \phi_L^{(x)})_{x=1,2}\Big) \\
&= \Big((\alpha_0^{(x)}(\beta_j^{(x)})^{I_j^{(l_j)}}, \alpha_1^{(x)}, \alpha_2^{(x)}, \beta_{j+1}^{(x)}, \ldots, \beta_L^{(x)})_{x=1,2}\Big) \\
&= \Big(((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{s_1^{(x)}} f^{s_2^{(x)}}, g^{s_1{}^{(x)}}, g^{s_2{}^{(x)}}, h_{j+1}^{s_1{}^{(x)}}, \ldots, h_L^{s_1{}^{(x)}})_{x=1,2}\Big).
\end{aligned}
$$

In re-randomization procedure we set,

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

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

$$
\begin{aligned}
sk^{(r)}_{u,v_i^{(l_i)},v_j^{(l_j)}} &= \Big(((\theta_0^{(1)})^{\gamma_x}(\theta_0^{(2)})^{\delta_x}, (\theta_1^{(1)})^{\gamma_x}(\theta_1^{(2)})^{\delta_x}, (\theta_2^{(1)})^{\gamma_x}(\theta_2^{(2)})^{\delta_x}, \\
&\qquad (\phi_{j+1}^{(1)})^{\gamma_x}(\phi_{j+1}^{(2)})^{\delta_x}, \ldots, (\phi_L^{(1)})^{\gamma_x}(\phi_L^{(2)})^{\delta_x})_{x=2,3}\Big). \\
&= \Big(((v\prod_{k=i}^{j} h_k^{I_k^{(l_k)}})^{\widetilde{s}_1^{(x)}} f^{\widetilde{s}_2^{(x)}}, g^{\widetilde{s}_1^{(x)}}, g^{\widetilde{s}_2^{(x)}}, h_{j+1}^{\widetilde{s}_1^{(x)}}, \ldots, h_L^{\widetilde{s}_1^{(x)}})_{x=1,2}\Big).
\end{aligned}
$$

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

Algorithm 6 Encrypt

input: Public key 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 $(I_i^{(l_i)}, \ldots, I_{j-1}^{(l_{j-1})}, I_j^{(l_{j1})}; I_j^{(l_{j2})})$ be the node identity of
       the corresponding chain $(v_i^{(l_i)}, \ldots, v_j^{(l_j)})$ or $(v_i^{(l_i)}, \ldots, v_j^{(l_{j1})}; v_j^{(l_{j2})})$ 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 $J = v_j^{(l_{j1})} + v_j^{(l_{j2})}$, then compute
            $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j1})}+I_j^{(l_{j2})}})^s.Z_3\Big)$.

        if $J = v_j^{(l_{j1})}$, then compute
            $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j1})}})^s.Z_3\Big)$.

        if $J = v_j^{(l_{j2})}$, then compute
            $C_x = \Big((M\|K).E^s, G^s.Z_1, F^s.Z_2, (V.\prod_{k=i}^{j-1} H_k^{I_k^{(l_k)}} H_j^{I_j^{(l_{j2})}})^s.Z_3\Big)$.

        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 $\mu$ to compute $C_\mu = \{C_{\mu(1)}, C_{\mu(2)}, ..C_{\mu(l)}\}$.
     Broadcast ciphertext $\mathsf{CT}$=$\{k, K, C_\mu\}$.
```

Remark 2. *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$\{\frac{N}{3}, N-r, 2r-1\}$.

Algorithm 7 Decrypt

```
input: $\mathsf{PK}$, $\mathsf{CT}=\{k, K, C_\mu\}$, $sk_u = \{sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_2})}}, sk_{u,v_i^{(l_i)},v_j^{(l_{j_1})}+v_j^{(l_{j_2})}} | 1 \leq i \leq L-1, i+1 \leq j \leq L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$
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 mecha-
             nism 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 $2 \cdot 3 + 2 \cdot 3^2 + \ldots + 2 \cdot 3^k$ 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 $2\cdot 3+2\cdot 3^2+\ldots+2\cdot 3^k-3k=3\cdot(3^k-1)-3k\leq 3^{k+1}-3k$ subset difference sets. This gives the maximum number of subsets in which it can belong, is $\sum\limits_{k=1}^{\log_3 N}(3^{k+1}-3k)=O(N)$. 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 Figure 1, $\mathsf{PN}(v_4^{(16)})=\{v_1^{(1)},v_2^{(2)},v_3^{(6)},v_4^{(16)}\}$ 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 $\mathsf{Decrypt}$ 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 coreresponding 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 $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$, $sk_{u,v_i^{(l_i)},v_j^{(l_{j1})}+v_j^{(l_{j2})}}$ for $(I_i^{(l_i)},\ldots,I_{j-1}^{(l_{j-1})}\ ,I_j^{(l_j)})$, $(I_i^{(l_i)},\ldots,I_{j-1}^{(l_{j-1})},I_j^{(l_{j1})}+I_j^{(l_{j2})})$ 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 $S_{v_1^{(1)},v_4^{(2)}+v_4^{(3)}}$.

Correctness: 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 $sk_{u,v_i^{(l_i)},v_j^{(l_j)}}$.

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

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 using the corresponding 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. *Our scheme 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. □

5 Security Analysis

Theorem 1. *Our OAnoBE scheme described in section 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: $\mathsf{Game}_\mathsf{h}^0(0 \le h < l_0)$,$\mathsf{Game}_{\mathsf{l_0}}^0$, $\mathsf{Game}_{\mathsf{l_1}}^1$,$\mathsf{Game}_\mathsf{k}^1$ $(l_1 > k \ge 1)$ 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

$$\mathsf{ID_{i,0}} = (0, \ldots, 0, I_i^{(l_i)}, I_{i+1}^{(l_{i+1})}, \ldots, I_j^{(l_j)}, 0, \ldots, 0) = (I_1^{(l_1)}, I_2^{(l_2)}, \ldots, I_L^{(l_L)}).$$

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.

• 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 6. $\mathcal{C}$ 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 6.

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, $1 \leq i \leq l_1 - k$ as encryption of m_1 for identity $\mathsf{ID_{i,1}}$ and C_i, $l_1 - k + 1 \leq i \leq l$ as $(R_1, R_2, R_3, R_4) \in_R \mathbb{G}_T \times \mathbb{G}^3$ following Algorithm 6. $\mathcal{C}$ 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^0_{h-1} and Game^0_h, $1 \leq h \leq l_0$ are indistinguishable if L-wDBDHI*, BSD and L-cDDH assumption holds. Game^1_{k-1} and Game^1_k, $2 \leq k \leq l_1$ are indistinguishable by Lemma 4 under the same assumptions. Let the adversary's advantage of winning Game^0_h is Adv^0_h, and that of Game^1_k is Adv^1_k. Let the adversary's advantage of distinguishing Game^0_h, Game^0_{h-1} and Game^0_k, Game^0_{k-1} is at most ϵ. Then advantage of distinguishing Game^0_0, Game^1_1 is given by

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

□

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

Proof. To prove the indistinguishability of Game^0_{h-1} and Game^0_h, we define $\overline{\mathsf{Game}}^0_h$ in slightly different way from $\mathsf{Game^0_h}$ and prove the indistinguishability of $\overline{\mathsf{Game}}^0_{h-1}$ and $\overline{\mathsf{Game}}^0_h$. For $i = l_0 - h + 1$ to l, the generated challenged ciphertext in $\overline{\mathsf{Game}}^0_h$ 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: $\overline{\mathsf{Game}}^0_{h-1}$ and $\overline{\mathsf{Game}}^0_h$ are indistinguishable under L-wDBDHI* assumptions.
Proof. Let there is an adversary $\mathcal{A}$ that can distinguish $\overline{\mathsf{Game}}^0_{h-1}$ and $\overline{\mathsf{Game}}^0_h$ 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

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

So, some $I_k^{(\bar{l}_k)}$ may be 0 at the beginning and end. Compute $G = g_p.R_g, F = g_p^z.R_f, V = g_p^y.\prod_{k=1}^{L}(A_{L-k+1})^{I_k^{(\bar{l}_k)}} R_v, H_k = g_p^{x_k}/A_{L-k+1}R_{h,k}$ $(1 \leq k \leq L)$, $E = e(A_1, A_L g_p^\gamma)$, 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 $T_{v_j^{(l_j)}}$ 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 $I_s^{(\bar{l}_s)} \neq I_s^{(l_s)^*}$.

   i. Take $r_1, r_2 \in_R \mathbb{Z}_n$ and implicitly set $\overline{r}_1 = r_1 + \frac{\alpha^s}{I_s^{(l_s)^*} - I_s^{(\bar{l}_s)}}$. 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

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

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

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

   As all the required $A_k, I_k^{(l_k)^*}, x_k$ 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 $w.(v\prod_{k=1}^{s} h_k^{I_k^{(l_k)^*}})^{\overline{r}_1}. f^{r_2}$ is also computable.

   iii. Now using Derive algorithm as stated in Algorithm 5, $\mathcal{C}$ computes first component of $sk^{(d)}_{i, v_i^{(l_i)}, v_j^{(l_j)}}$ as $w.(v\prod_{k=1}^{j} h_k^{I_k^{(l_k)^*}})^{\overline{r}_1} f^{r_2}$. Other components $(g^{\overline{r}_1}, g^{r_2}, h_{j+1}^{\overline{r}_1}, \ldots, h_L^{\overline{r}_1})$ 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 $m_0 = (M_0||K), m_1 = (M_1||K)$ to $\mathcal{C}$, where last k bits of each message is K. $\mathcal{C}$ computes ciphertext components following Algorithm 6 as follows. For $1 \leq i \leq l_0 - h + 1$, 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 $l_0 - h + 2 \leq i \leq l$, 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

$$\begin{aligned}
C_i &= \Big(m_o.E^s, G^s.Z_1, F^s.Z_2, (V\prod_{k=1}^{L} H_k{}^{I_k^{(l_k)}})^s.Z_3\Big), 1 \leq i \leq l_0 - h \\
C_i &= \Big(m_0.E^s.T, G^s.Z_1, F^s.Z_2, (V\prod_{k=1}^{L} H_k{}^{I_k^{(l_k)}})^s.Z_3\Big), l_0 - h + 2 \leq i \leq l \\
C_{l_0-h+1} &= \Big(m_0.T.e(A_1, h^\gamma), h.Z_1, h^z.Z_2, h^{y+\sum_{k=1}^{L} I_k^{(l_k)}.x_k}.Z_3\Big), \\
&\quad \text{where } Z_1, Z_2, Z_3 \in_R \mathbb{G}_q, s \in_R \mathbb{Z}_n, T \in_R \mathbb{G}_{T,p}.
\end{aligned}$$

$\mathcal{C}$ 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

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

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 $\overline{\mathsf{Game}}_h^0$, 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. (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_{h-1}^0 and Game_h^0 are indistinguishable under same assumptions. □

Lemma 4. Game_{k-1}^1 *and* Game_k^1 *are indistinguishable under L-wDBDHI*, BSD and L-cDDH assumptions.*
The proof of this Lemma is analogous to that of Lemma 3.

6 Special Variant of Our Scheme

Let $\{v_L^{(l_i)} | 1 \leq l_i \leq N\}$ be leaf nodes of a tree. We fix $\{v_L^{(l_i)} |\ l_i = 1, 9i, 9i+1, 1 \leq i \leq \lfloor N/9 \rfloor\}$ 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 $\mathsf{ST}(\mathrm{R})$, 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 $\mathsf{ST}(\mathrm{R})$, 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 $\mathsf{ST}(\mathrm{R})$, 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 $sk_u = \{sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_2})}}, sk_{u, v_i^{(l_i)}, v_j^{(l_{j_1})} + v_j^{(l_{j_2})}} | L - 2 \leq i \leq L - 1, i + 1 \leq j \leq L, v_i^{(l_i)} \in \mathsf{PN}(v_L^{(l_L)}), v_j^{(l_{j_1})}, v_j^{(l_{j_2})} \in \mathsf{HN}(v_L^{(l_L)})\}$. On decryption time user uses these secret keys to decrypt l ciphertext component. So decryption attempt is at most $O(l)$.

Example: For Figure 4, 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.

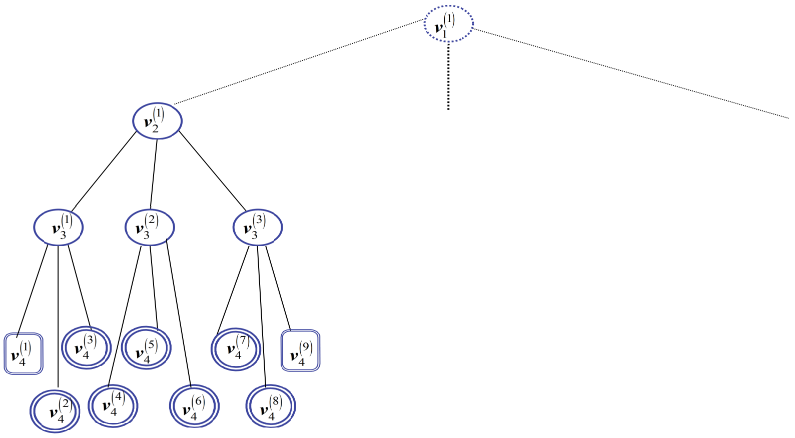

Figure 4: First 9 nodes in a tree with revoked user at $\{v_4^{(1)}, v_4^{(9)}\}$

7 Conclusion

We have designed an efficient outsider-anonymous broadcast encryption in public key setting employing *ternary tree subset difference* method, achieving revocation property which is one of the most significant requirement in broadcast encryption setting. The ciphertext size is significantly reduced as compared to existing similar work in standard model. 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. 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 $\mathsf{min}\{\frac{N}{k}, N-r, 2r-1\}$. However, the decryption cost will be increased.

References

Acharya, K. and Dutta, R. (2016). *Secure and Efficient Construction of Broadcast Encryption with Dealership*, pages 277–295. Springer International Publishing, Cham.

Barth, A., Boneh, D., and 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*, FC'06, pages 52–64, Berlin, Heidelberg. Springer-Verlag.

Bhattacherjee, S. and Sarkar, P. (2015). Tree based symmetric key broadcast encryption. *J. of Discrete Algorithms*, 34(C):78–107.

Boneh, D., Gentry, C., and 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*, CRYPTO'05, pages 258–275, Berlin, Heidelberg. Springer-Verlag.

Boneh, D. and Hamburg, M. (2008). Generalized identity based and broadcast encryption schemes. In Pieprzyk, J., editor, *Advances in Cryptology - ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 455–470. Springer Berlin Heidelberg.

Boneh, D., Sahai, A., and Waters, B. (2006). Fully collusion resistant traitor tracing with short ciphertexts and private keys. In Vaudenay, S., editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 573–592. Springer Berlin Heidelberg.

Boneh, D. and Silverberg, A. (2003). Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324(1):71–90.

Boneh, D. and Waters, B. (2006). A fully collusion resistant broadcast, trace, and revoke system. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 211–220, New York, NY, USA. ACM.

Boneh, D., Waters, B., and Zhandry, M. (2014). Low overhead broadcast encryption from multilinear maps. In Garay, J. and Gennaro, R., editors, *Advances in Cryptology - CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 206–223. Springer Berlin Heidelberg.

Boneh, D. and Zhandry, M. (2014). Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In Garay, J. and Gennaro, R., editors, *Advances in Cryptology CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 480–499. Springer Berlin Heidelberg.

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

Coron, J.-S., Lepoint, T., and Tibouchi, M. (2013). Practical multilinear maps over the integers. In Canetti, R. and Garay, J., editors, *Advances in Cryptology CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 476–493. Springer Berlin Heidelberg.

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*, ASIACRYPT'07, pages 200–215, Berlin, Heidelberg. Springer-Verlag.

Delerablée, C., Paillier, P., and Pointcheval, D. (2007). Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In Takagi, T., Okamoto, T., Okamoto, E., and Okamoto, T., editors, *Pairing*, volume 4575 of *Lecture Notes in Computer Science*, pages 39–59. Springer.

Fazio, N. and Perera, I. (2012). Outsider-anonymous broadcast encryption with sublinear ciphertexts. In Fischlin, M., Buchmann, J., and Manulis, M., editors, *Public Key Cryptography PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 225–242. Springer Berlin Heidelberg.

Fiat, A. and Naor, M. (1994). Broadcast encryption. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '93, pages 480–491, New York, NY, USA. Springer-Verlag New York, Inc.

Fukushima, K., Kiyomoto, S., Tanaka, T., and Sakurai, K. (2009). Ternary subset difference method and its quantitative analysis. In *Information Security Applications*, pages 225–239. Springer.

Garg, S., Gentry, C., and Halevi, S. (2013a). Candidate multilinear maps from ideal lattices. In Johansson, T. and Nguyen, P., editors, *Advances in Cryptology EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17. Springer Berlin Heidelberg.

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

Gentry, C. (2006). Practical identity-based encryption without random oracles. In *Proceedings of the 24th Annual International Conference on The Theory and Applications of Cryptographic Techniques*, EUROCRYPT'06, pages 445–464, Berlin, Heidelberg. Springer-Verlag.

Gritti, C., Susilo, W., Plantard, T., Liang, K., and Wong, D. (2015). Broadcast encryption with dealership. *International Journal of Information Security*, pages 1–13.

Halevy, D. and Shamir, A. (2002). The lsd broadcast encryption scheme. In Yung, M., editor, *Advances in Cryptology CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer Berlin Heidelberg.

He, K., Weng, J., Liu, J.-N., Liu, J. K., Liu, W., and Deng, R. H. (2016). Anonymous identity-based broadcast encryption with chosen-ciphertext security. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 247–255, New York, NY, USA. ACM.

Lewko, A., Sahai, A., and Waters, B. (2010). Revocation systems with very small private keys. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 273–285.

Libert, B., Paterson, K., and Quaglia, E. (2012). Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In Fischlin, M., Buchmann, J., and Manulis, M., editors, *Public Key Cryptography - PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 206–224. Springer Berlin Heidelberg.

Liu, W., Liu, J., Wu, Q., and Qin, B. (2014). Hierarchical identity-based broadcast encryption. In Susilo, W. and Mu, Y., editors, *Information Security and Privacy*, volume 8544 of *Lecture Notes in Computer Science*, pages 242–257. Springer International Publishing.

Liu, W., Liu, J., Wu, Q., Qin, B., and Li, Y. (2015). Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption. *International Journal of Information Security*, pages 1–16.

Naor, D., Naor, M., and Lotspiech, J. (2001). Revocation and tracing schemes for stateless receivers. In Kilian, J., editor, *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer Berlin Heidelberg.

Phan, D. H., Pointcheval, D., Shahandashti, S., and Strefler, M. (2013). Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4):251–265.

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

Sakai, R. and Furukawa, J. (2007). Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217.

Seo, J. H., Kobayashi, T., Ohkubo, M., and Suzuki, K. (2009). *Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts*, pages 215–234. Springer Berlin Heidelberg, Berlin, Heidelberg.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In Blakley, G. and Chaum, D., editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Berlin Heidelberg.

Wu, Q., Qin, B., Zhang, L., and Domingo-Ferrer, J. (2011). Fully distributed broadcast encryption. In Boyen, X. and Chen, X., editors, *Provable Security*, volume 6980 of *Lecture Notes in Computer Science*, pages 102–119. Springer Berlin Heidelberg.

Zhang, M. and Takagi, T. (2013). Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group e-mail systems with privacy preservation. *IEEE Systems Journal*, 7(3):410 – 419.