Journal of Information Hiding and Multimedia Signal Processing ©2024 ISSN 2073-4212
Ubiquitous International Volume **15**, Number **4**, December **2024**

Efficient Identity Based Broadcast Encryption Scheme with Permanent Revocation

Hisham Dahshan

College of Computing & Information Technology,
Arab Academy for Science Technology and Maritime Transport, Cairo, Egypt
hishamdahshan@aast.edu

Eslam Abdel Haleem Ali

Department of Communications
The Military Technical College
Alkhalifa Almamoun st, Cairo, Egypt
eslamsnono45@gmail.com

Yahya Z. Mohasseb

College of Engineering & Technology
Arab Academy for Science Technology and Maritime Transport, Cairo, Egypt
ymohasseb@aast.edu

Received July 25, 2024, revised November 4, 2024, accepted November 5, 2024.

Abstract. *Broadcast encryption (BE) schemes enable the sender of a message to determine a subset of users to which the message will be encrypted. Permanent revocation is very crucial in many applications. Any corrupted user whose keys were compromised, can help the attackers to receive sensitive data. This paper proposes two schemes to obtain an efficient broadcast encryption. The first proposed scheme is an enhanced identity based broadcast encryption (IBBE). The complexity of the IBBE scheme is $O(n)$, where n is the maximum number of users. In addition, a permanent revocation scheme for identity-based broadcast encryption (RIBBE) is proposed. In the proposed RIBBE scheme, permanent revocation is achieved where a trusted authority periodically broadcasts the updating parameters and revocation list (RL) at time T. Only valid users can retrieve updating parameters and update their keys using these parameters. In RIBBE, the updated key is constant, but the private and public keys are not constant. Each time a revocation is performed, the private and public keys get shorter by $O(n - R)$ where n is the total number of users and R is the number of revoked users.*
Keywords: Pairing Based Cryptography, Identity based Encryption, Revocation

1. **Introduction.** One of the branches of cryptography is broadcast encryption. Broadcast encryption gives users one of the most important features in communication which is the ability for broadcasting messages. One of the main problems here is, what if we need to broadcast to specific users and revoke the others from understanding the message.

So, Revocation is a big deal in BE. Revocation can be categorized into two types which are: Temporary revocation, and Permanent revocation. Temporary revocation means that a user can select some users and exclude the others from retrieving the message. But those excluded users are still have the ability to retrieve messages if they are included in any other broadcast transmission. Permanent revocation means that some of users that may be expired or corrupted are revoked from the users group. This is done by updating

keys of the valid users only. So, revoked users now can't use their keys to get or retrieve any data. The main problems in permanent revocation are:

- How to update keys without allowing revoked users from getting the new keys.
- The transmission cost of new keys is very vital so, it is required to make both the elements of private key and update key constant.
- Updating keys for permanent revocation requires that all users have to be online all the time (stateful receivers).

Therefore, implementing an efficient revocation mechanism which can support large number of users is crucial because it prohibits unauthorized user from retrieving important data by revoking a user's private key. There are several studies that deal with certificate revocation in public key encryption (PKE) [1],[2]. In public-key encryption systems that use the PKI, it is easy to revoke a user through revoking his certificate. In identity-based encryption (IBE) [3], a revocation process is different, a trusted authority periodically updates the private key for a user at time T. So, this mechanism in IBE requires:

- Receivers and trusted authority work in stateful mode (means to be online all the time).
- A secure channel must be existed to transmit the updated keys.

In this paper, a permanent revocation scheme for identity based broadcast encryption through open networks (RIBBE) is proposed. The proposed revocation encryption system uses multilinear mapping. The proposed RIBBE scheme tries to figure out the following problems: (1) keeping the updated keys secret from revoked users and any other collusion. (2) making private key parameters and updated keys parameters shorter and constant.

2. **Related Work.** The broadcast encryption research was launched in Berkovits [4] and Fiat and Naor [5]. Most of BE revocation schemes fall into one of two categories: tree-based constructions, and secret-sharing constructions [6].

Tree-based revocation schemes were proposed in many schemes [7], [8] with stateless and stateful receivers. Few of stateful schemes are based on logical key hierarchy [LKH] [7].

In LKH schemes, every user keeps an order of $log(n)$ keys while the center authority (CA) keeps a tree of keys. When a user is revoked, the CA must modify the keys of the tree path from the revoked user's leaf to the root. So, a message revoking a single user consists of $O(log(n))$ keys. A disadvantage of the LKH schemes is that users must update their keys whenever the group key is changed (either when users are added or revoked).

Secret sharing has been used in many schemes "i.e. " Naor and Pinkas [9]. They used secret sharing method to revoke up to t users. The scheme is theoretically secure against a group of adversaries of size $k = t$, where k is an upper bound on the group size (number of keys) the adversary can compromise. The user computation cost is $O(t^2)$.

An IBE scheme that introduces a revocation scheme (RIBE) was presented by Boldyreva, Goyal, and Kumar [10]. This scheme uses a tree based revocation and the attribute-based encryption [ABE] [11], [12]. Using tree-based revocation has a drawback that neither the number of private keys nor the number of update key elements are constant [13].

3. **CONTRIBUTIONS.** The proposed scheme enables the system to revoke users permanently without the need for a third party. As a result of updating keys of valid users, backward and forward secrecy are achieved in the proposed scheme. The proposed scheme performs permanent revocation with low computation cost in the computation of public and private keys with complexity $\mathcal{O}(n - R)$. The proposed scheme has been implemented

using the open source library Pairing-Based Cryptography (PBC)[14]. The execution time of algorithms used in the proposed scheme has been computed to show that the theoretical analysis is consistent with the experimental analysis.

4. **The proposed IBBE.** This section explains the model of the proposed IBBE scheme and defines its algorithms. Also, it defines the correctness of the proposed scheme.

4.1. **Model of The Proposed Scheme.** The proposed scheme consists of five algorithms (ParaGen, Extract, Setup, Encrypt, Decrypt) as follows:

- **ParaGen (λ, n):** Let the maximum number of users be n and the security parameter is λ. Let the tulpe $\Psi = (q, \mathbb{G}, \mathbb{G}_T, e) \leftarrow PairGen(1^\lambda)$ where $\mathbb{G}$ is an additive cyclic sub group of prime order r in the $E(F_q)$ and $\mathbb{G}_T$ is a multiplicative subgroup in the field F_{q^k}. The pairing function is $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. The master secret key (s) is generated where $s \in \mathbb{Z}_q^*$, and a random element g is selected such that g $\in \mathbb{G}$ and g is a generator for $\mathbb{G}$. A hash function is $Hash : \{0,1\}^* \rightarrow \mathbb{G}$. The $PK = (pk_0, ..., pk_n)$ where:

$$pk_i = (R_i, A_i) \tag{1}$$
$$R_i = g^{-r_i} \quad \text{where} \quad r_i \in \mathbb{Z}_q \tag{2}$$
$$A_i = e(x_i, g) \quad \text{where} \quad x_i \in \mathbb{G} \tag{3}$$

  Where $0 \leq i \leq n$. The proposed scheme system parameters is $\pi = (\lambda, n, \Psi, \text{g}, s, Hash, PK)$.
- **Extract(**g, x_i, r_i, U_j, ID_j, s**):** This algorithm is run by a trusted authority (it can be a distribution center for any of the services that use BE like a pay-tv). It ensures that each valid user gets the required parameters for broadcasting and receiving. It takes as input: s, x_i, r_i, U_j , ID_j where ($0 \leq i \leq n$, $1 \leq j \leq n$, and $i \neq j$) for each user U_j. It ouputs: γ_i, $\alpha_{i,j}$, and α_j as follows:

$$\gamma_i = \{x_0, ..., x_{j-1}, x_{j+1}, ...x_n\} \tag{4}$$
$$\alpha_j = Hash(ID_j)^s \tag{5}$$
$$\alpha_{i,j} = Hash(ID_j)^{r_i \cdot s} \tag{6}$$

- **Setup(**ID_j, $Hash$, s, $\alpha_{i,j}$, γ_i**):** Each user j computes his decryption key d_j (Member Decryption Key) using γ_i, and $\alpha_{i,j}$ where $0 \leq i \leq n$ and $1 \leq j \leq n$ as follows:

$$\begin{gathered} d_j = (\beta_{0,j}, ..., \beta_{j-1,j}, ..., \beta_{n,j}) \quad where \\ \beta_{i,j} = \gamma_i \alpha_{i,j} \quad and \quad 0 \leq i \leq n \quad and \quad i \neq j \end{gathered} \tag{7}$$

- **Encrypt(** S, PK, M**):** Any one has the group encryption key can now broadcast an encrypted message to a specific users. The sender firstly selects the receivers group $S \subseteq \{1, ..., n\}$, then he computes the following:
  1. Let $\overline{S} = \{0, 1, ..., n\} \backslash S$, then chooses t randomly from $\mathbb{Z}_q^*$ and computes the session key (ξ) as follows:
$$\xi = (\prod_{i \in \overline{S}} A_i)^t \tag{8}$$
  2. The overhead messages of ciphertext c_1, c_2 are calculated as follows:
$$c_1 = g^t \tag{9}$$
$$c_2 = (\prod_{i \in \overline{S}} R_i)^t \tag{10}$$
  3. The plain text message M will be encrypted and the ciphertext packet (S, c_1, c_2, c) will be broadcasted by the sender where:
$$c = Enc_\xi(M) \tag{11}$$

If no users have been revoked, the scheme calculates the session key using (R_0, A_0). Also, (R_0, A_0) will be the public key.

- **Decrypt(S, U_j, s_j, d_j, c):** The user checks if his ID (U_j) is in the receivers set S, i.e. $j \in S$. If he is a valid user, then he uses d_j, and α_j along with the overhead of the ciphertext messages c_1, c_2 to derive the decryption key ξ as the follows:

$$\xi = e(\prod_{i \in \overline{S}} \beta_{i,j}, c_1).e(\alpha_j, c_2) \tag{12}$$

Then, the user uses the session key ξ to recover the original message M by decrypting the ciphertext c.

4.2. **Correctness Proof.** The scheme correctness implies that for any user needs to broadcast an encrypted message CT where $CT \leftarrow Encrypt(S, PK, M)$ to a set of users, then the valid users can get the message M where $M \leftarrow Decrypt(\alpha, U_j, ID_j, S, d_j, CT)$.

Definition 4.1. *The Scheme should fulfill the following correctness requirements:*
For all $\pi \leftarrow ParaGen(\lambda, n)$, $(\alpha, \gamma, PK) \leftarrow Extract(\pi, U_j, ID_j)$, $d_j \leftarrow Setup(\alpha, \gamma)$, $CT \leftarrow Encrypt(S, PK, M)$, *we have* $M \leftarrow Decrypt(\alpha, U_j, ID_j, S, d_j, CT)$.

The correctness is derived as follows:

$$\begin{aligned}
&e(\prod_{i \in \overline{S}} \beta_{i,j}, c_1).e(\alpha_j, c_2) \\
&= e(\prod_{i \in \overline{S}} \beta_{i,j}, g^t).e(\alpha_j, (\prod_{i \in \overline{S}} R_i)^t) \\
&= e(\prod_{i \in \overline{S}} X_i Hash(ID_j)^{(r_i s)}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i \in \overline{S}} g^{-r_i})^t) \\
&= e(\prod_{i \in \overline{S}} X_i, g^t).e(\prod_{i \in \overline{S}} Hash(ID_j)^{(r_i s)}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i \in \overline{S}} g^{-r_i})^t) \\
&= e(\prod_{i \in \overline{S}} X_i, g^t).e(Hash(ID_j)^{s \sum_{i \in \overline{S}} r_i}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i \in \overline{S}} g^{-r_i})^t) \\
&= e(\prod_{i \in \overline{S}} X_i, g^t).e(Hash(ID_j)^{s \sum_{i \in \overline{S}} r_i}, g^t).e(Hash(ID_j)^{(s)}, g^{t \sum_{i \in \overline{S}} -r_i}) \\
&= e(\prod_{i \in \overline{S}} X_i, g^t) \\
&= \xi
\end{aligned} \tag{13}$$

Then, the user uses the session key ξ to obtain the original message M by decrypting the ciphertext c as follows:

$$M = Dec_\xi(c) \quad \text{Where, c is the ciphertext} \tag{14}$$

4.3. **Theoretical Analysis.** Evaluation Parameters can be splitted into offline parameters and online parameters. The offline parameters are the complexity of algorithms that can be done without any need for users to be online such as setup and extract algorithms. The online parameters are the complexity of algorithms when users are online such as Encrypt and Decrypt algorithms.

In our proposed scheme, from equations 1, 2 and 3, it can be concluded that each user stores $(n+1)$ pair of elements for the PK (One element is in $\mathbb{G}$ and the other element is in $\mathbb{G}_{\mathbb{T}}$). The user is able now to encrypt any message for a specific set of receivers and broadcast it. From equation 8, the user has to perform two exponentiation operations in $\mathbb{G}$ to generate the session key ξ. Then, the user uses that session key in symmetric encryption algorithm to generate the ciphertext and the corresponding overhead that will be used for retrieving the session key and hence, to decrypt ciphertext. The proposed scheme generates short and constant overhead c_1, c_2 (both are in $\mathbb{G}$).

Every user saves n elements in $\mathbb{G}$ for the member decryption key d_j (equation 7) and only one element in $\mathbb{G}$ for the private key α_j (equation 5). So, the stored keys PK, d_j at each user are $\mathcal{O}(n)$.

The contributory broadcast encryption scheme (CBE) [15] has computation cost of $O(n^3)$ and it has transmission cost of $O(n^3)$. If a user will be revoked from a set, all the parameters and sets will need to be rearranged and regenerated. The transmission and computation cost of the proposed IBBE scheme at setup algorithm is $O(n^2)$.

The extract algorithm for each user computes n elements $(\gamma_i,\ \alpha_{i,j})$. Therefore, its computation cost is $\mathcal{O}(n)$. The computation cost of the setup algorithm of the proposed scheme is $O(n)$. There is no transmission cost in the setup algorithm as each user extracts all the required data from the trusted authority.

To add a new user in our IBBE scheme, the trusted authority (TA) sends to all current users the elements which are related to the new user. Then, TA extracts the required elements for the new user. In the proposed IBBE scheme, no data is sent over open network. But, in ordr to add a new user, TA publishes R_{n+1}, A_{n+1} to all users. Also, TA publishes γ_{n+1}, $\alpha_{n+1,j}$ which are used to derive $\beta_{n+1,j}$ for all users where $1 \leq j \leq n$. Both the transmission and computation cost of adding a new user in the proposed IBBE scheme is $\mathcal{O}(n)$. On the other hand, CBE [15] current users perform $\mathcal{O}(n^3)$ computation, and transmission operations in order to add the new user.

To compare our proposed IBBE scheme in transmission and computation cost with CBE [15], and Li et al. scheme [17], Table 1 presents the computation, and transmission cost for set up, session key derivation, and adding new users.

Table 1. Computations and transmissions cost Comparison

Item	**Proposed**	**CBE**[15]	**IBBE**[17]
User recruitment	**yes**	**yes**	**yes**
Permanent revocation	**yes**	**no**	**no**
Set up Transmission cost	**null**	$O(n^3)$	$O(n^2)$
Set up Computation cost	$O(n)$	$O(n^3)$	$O(n^2)$
Computation cost for encryption session key derivation	$O(\overline{S}^2)$	$O(\overline{S}^2)$	$O(\overline{S}^2)$
Computation cost for decryption session key extraction	$O(\overline{S}^2)$	$O(\overline{S}^2)$	$O(\overline{S}^2)$
Add new user transmission cost	$O(n)$	$O(n^3)$	$O(n)$
Add new user computation cost	$O(n)$	$O(n^3)$	$O(n)$

5. **The Proposed Revocation Identity-based Broadcast Encryption Scheme (RIBBE).** In this section, our proposed revocation identity-based broadcast encryption echeme (RIBBE) is presented.

5.1. **Scheme Description.** The revocation process in the proposed RIBBE scheme is shared between the trusted authority and the users. The proposed RIBBE scheme consists of a tuple of algorithms (Setup, Encrypt, Decrypt, Revoke). The setup and encrypt algorithms are in the trusted authority side. The decrypt and revoke algorithms are in the client side. Figure 1 illustrates the proposed RIBBE scheme at the TA side, and at the client side. It is assumed that the parameters $\pi = (n, \lambda, \mathrm{g}, s, \Psi, Hash)$ have been already generated before at the trusted authority during the IBBE scheme. The proposed RIBBE scheme algorithms are as follows:

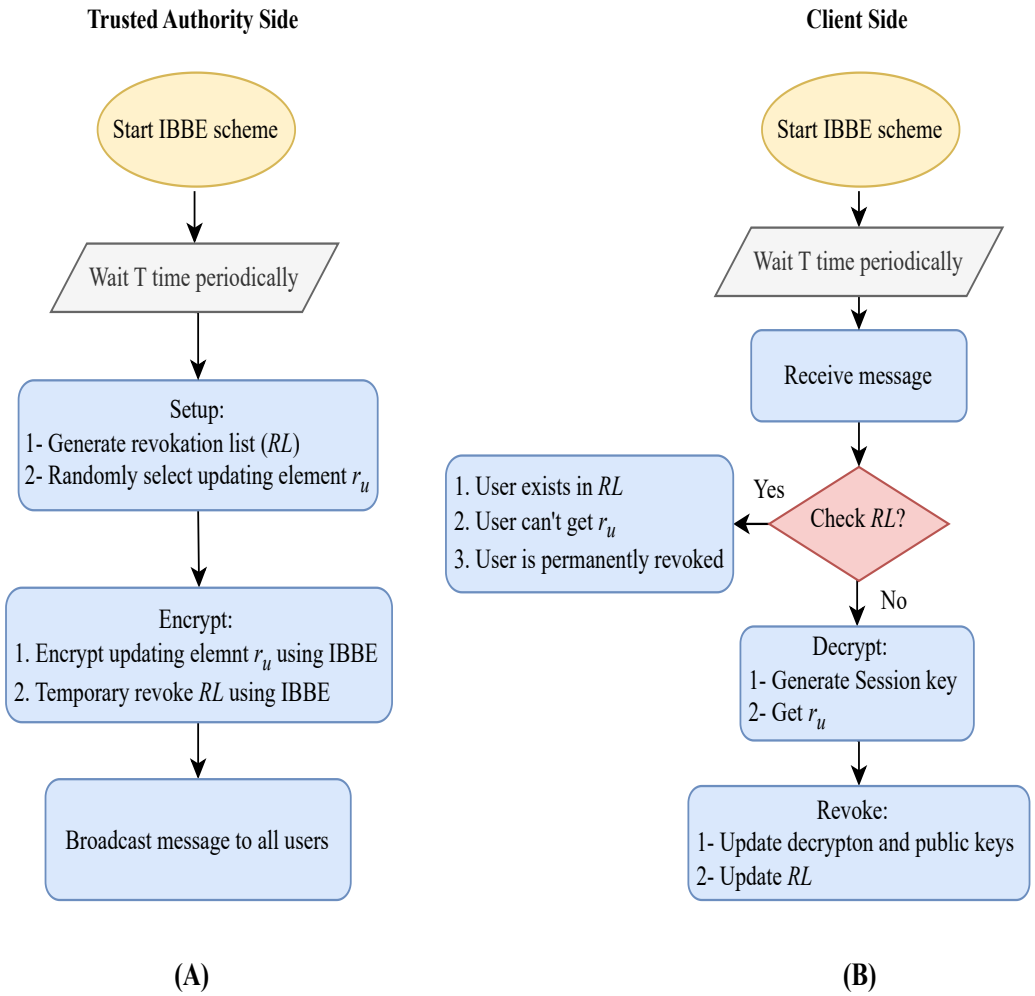

FIGURE 1. The proposed RIBBE scheme: (A) TA Side, (B) Client Side

- **Setup (S):** The trusted authority (TA) performs two steps as follows:
  - First step: it selects an element randomly $r_u \in \mathbb{Z}_q^*$.
  - Second step: it constructs the revocation list (RL) where RL is $\overline{S} = \{0, 1, ..., n\} \backslash S$ (those users who will be revoked permanently).
- **Encrypt (RL, PK, r_u):** TA selects the valid users $S \subseteq \{1, ..., n\}$, then perform the encryption process to encrypt r_u (Only valid users will have the ability to retrieve r_u):

– Let $RL = \overline{S} = \{0, 1, ..., n\} \backslash S$. TA selects t randomly such that $t \in \mathbb{Z}_q^*$, then calculates the session key (ξ) as follows:

$$\xi = (\prod_{i \in \overline{S}} A_i)^t \tag{15}$$

– Computes the overhead of the ciphertext c_1, c_2 where:

$$c_1 = g^t \tag{16}$$

$$c_2 = (\prod_{i \in \overline{S}} R_i)^t \tag{17}$$

– TA broadcasts the ciphertext (RL, c_1, c_2, c) where:

$$c = Enc_\xi(r_u) \tag{18}$$

- **Decrypt (α_j, S, U_j, d_j, c):** Each user verifies if $j \in S$. If he isn't revoked (i.e. he is a valid member of S), then he uses the last derived decryption key d_j alongside α_j, and the overhead of the ciphertext messages c_1, c_2 to generate the session key ξ as follows:

$$\xi = e(\prod_{i \in \overline{S}} \beta_{i,j}, c_1).e(s_j, c_2) \tag{19}$$

Then, he uses the session key ξ for decrypting the ciphertext message (c) (obtained in equation 18) to get r_u. Any revoked user will not be able to update his session key ξ as he can't retrieve r_u.

- **Revoke (r_u, RL):** First: each valid user now has to recalculate his decryption key d_j. Using RL, each valid user will omit any index i that exists in RL and computes the updated decryption key d_j as follows:

$$d_j = (\beta_{0,j}, ..., \beta_{j-1,j}, \beta_{j+1,j}, ..., \beta_{n,j}) \tag{20}$$
$$\text{where } i = \{0, 1, ..., n\} \backslash RL \text{ and } i \neq j$$

After revoking parameters of unauthorized users, each user now will recalculate $\beta_{i,j}$ using r_u where:

$$\beta_{i,j} = \gamma_i \, \alpha_{i,j}^{r_u} \tag{21}$$
$$\text{where } i = \{0, 1, ..., n\} \backslash RL \text{ and } i \neq j$$

Second, TA and each user update PK. They omit any index of unauthorized users from A_i, R_i where $i = \{0, 1, ..., n\}$. After revoking unauthorized index and using r_u, the new updated PK will be as follows:

$$PK = ((R_0, A_0), ...(R_n, A_n)) \tag{22}$$
$$\text{where } i = \{0, 1, ..., n\} \backslash RL \ , \ R_i = g^{-(r_i * r_u)} \text{ and } A_i = e(x_i, g)$$

After completing Revoke algorithm, all keys are updated. The PK of the system has been reduced as some of its elements which are related to unauthorized users indexes are revoked. Also, the derived decryption key for each user d_j is reduced. Now if any user needs to broadcast a message to any other group of valid users, he can use the IBBE scheme presented in section 4.

5.2. **Correctness.** The correctness of the proposed permanent RIBBE scheme implies that if all users (receivers and the sender) implement the scheme, then membes of the receiver set can always decrypt the ciphertext correctly and retrieve the RL and r_u. The proposed scheme correctness is defined as follows:

- For all $r_u \leftarrow Setup(S)$.
- For all $\overline{S}$, c_1, c_2, $Enc_\xi(r_u) \leftarrow Encrypt(RL, PK, r_u)$.
- For all $RL, r_u \leftarrow Decrypt(\alpha_j, S, U_j, d_j, c)$.
- For all RL, $\acute{d_j}$, $\acute{PK} \leftarrow Revoke(\overline{S}, r_u)$

It holds that $\xi \leftarrow Dec(S, \acute{d_j}, \acute{\alpha_j}, \acute{PK})$.

Extracting session key is still computable after updating keys. The generated session key $\xi = \prod_{i \in \overline{S}} A_i^t$ can still be extracted after updating keys. The proof of the proposed RIBBE correctness is as follows:

$$
\begin{aligned}
& e(\prod_{i\in\overline{S}} \beta_{i,j}, c_1).e(\alpha_j, c_2) = e(\prod_{i\in\overline{S}} \beta_{i,j}, g^t).e(\alpha_j, (\prod_{i\in\overline{S}} R_i)^t) \\
&= e(\prod_{i\in\overline{S}} x_i Hash(ID_j)^{((r_i * r_u)s)}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i\in\overline{S}} g^{-(r_i * r_u)})^t) \\
&= e(\prod_{i\in\overline{S}} x_i, g^t).e(\prod_{i\in\overline{S}} Hash(ID_j)^{((r_i * r_u)s)}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i\in\overline{S}} g^{-(r_i * r_u)})^t) \\
&= e(\prod_{i\in\overline{S}} x_i, g^t).e(Hash(ID_j)^{s\sum_{i\in\overline{S}}(r_i * r_u)}, g^t).e(Hash(ID_j)^{(s)}, (\prod_{i\in\overline{S}} g^{-(r_i * r_u)})^t) \\
&= e(\prod_{i\in\overline{S}} x_i, g^t).e(Hash(ID_j)^{s\sum_{i\in\overline{S}}(r_i * r_u)}, g^t).e(Hash(ID_j)^{(s)}, g^{t\sum_{i\in\overline{S}} -(r_i * r_u)}) \\
&= e(\prod_{i\in\overline{S}} x_i, g^t) \\
&= \xi
\end{aligned}
\tag{23}
$$

6. **Performance Analysis.** Performance analysis will include both theoretical and experimental analysis. The theoretical analysis is concerned with the complexity computation of the revocation scheme. The experimental analysis is simulating the revocation scheme and measuring time that a user takes to recompute his updated keys.

6.1. **Theoretical Analysis.** Park et al. scheme [16] has advantages over tree models that there is no need for the trusted authority to be online all the time. But, it has a disadvantage of having a multi-level multilinear mapping, which adds extra cost in computation for updating up the system when users are revoked.

The proposed scheme doesn't need multi-level multilinear mapping. The proposed scheme computation cost is the user cost for recomputing the keys after receiving the updating element. A user will update the keys based on the RL and will exclude any parameters related to any user inside the RL. So, the computation cost for keys recalculations will be $O(n - R)$. as shown in equation 20 where n is the total number of users, and R is the number of revoked users (users in RL). Also, it has a transmission cost of $O(1)$ as only a random element will be sent encrypted to update all keys.

Table 2 compares different revocation schemes according to the size of private keys (SK), public parameters (PP), update key (UK), type of revocation (Full or Selective), mapping (bilinear mapping (BLM) or multi linear mapping (MLM)), and the security assumptions. From Table 2, the proposed scheme has a constant update key. But each time a user is revoked, the public key PK and private key α_j get shorter by $|RL|$. A comparison with Park et al. scheme [16] deserves more concern. Park et al. scheme has private keys that have constant length but the public parameters aren't constant.

TABLE 2. Comparison of computational complexity for different schemes [16]

Scheme	SK size	PP size	UK size	model	Maps
BF[18]	$O(1)$	$O(1)$	$O(n-r)	Full	BLM
BGK[19]	$O(logn)$	$O(1)$	$O(rlog(n/r))$	Selective	BLM
LV[20]	$O(logn)$	$O(\lambda)$	$O(rlog(n/r))$	Full	BLM
SE[21]	$O(logn)$	$O(\lambda)$	$O(rlog(n/r))$	Full	BLM
LLP[22]	$O(log^{1}.5n)$	$O(1)$	$O(r)$	Full	BLM
RIBE-1[16]	$O(1)$	$O(n+\lambda)$	$O(1)$	Selective	MLM
RIBE-2[16]	$O(1)$	$O(logn+\lambda)$	$O(1)$	Selective	MLM
OUR	$O(n-r)$	$O(n-r)$	$O(1)$	Selective	MLM

However, Park et al. scheme has a high computation cost in re-keying because it is multi-level multi-linear mapping based scheme. In contrast, the proposed RIBBE scheme is more simple in updating keys. It only computes two exponentiations and one multiplication to update keys. Also, comparing to Park et al. scheme, each time users are revoked, shorter public parameters and shorter private keys are obtained in our proposed RIBBE scheme.

6.2. **Experimental Analysis.** Experimental analysis is done by simulating the proposed scheme. The implementation is done using a C-language library called Pairing based Cryptography Library [PCB-library] [14]. This library eases the implementation by offering different elliptic curves for pairing. The implementation uses Type-A pairing from the library. This needs two inputs for initializing the elliptic curve and pairing. The two inputs are as follows:

1. r-bits which is the length of the order of the subgroup $\mathbb{G} \subseteq E(F_q)$.
2. q-bits which is the length of the base prime of F_q.

For the purpose of simulation, two different cases for the input security parameters were selected as follows:

1. 1^{st} case : $r = 160\,bits$ and $q = 512\,bits$.
2. 2^{nd} case : $r = 256\,bits$ and $q = 1536\,bits$.

The embedding degree k of the type-A pairing elliptic curve is $k = 2$. So, the multiplicative group $\mathbb{G}_T$ will have $1024 - bit$ elements in the 1^{st}-case and will have $3072 - bit$ elements in the 2^{nd}-case.

The simulation has been done using a PC with Intel Core-i5 and 8 GB RAM. The implementation code were written in C-language under Linux. The simulation were done assuming that the total number of users $n = 200$. Each time the revoked users R differs such that the simulation is done for $R = \{3, 6, 30, 60, 90, 120, 150, 180\}$. Also, simulation were repeated $50 - times$ for each R and the average result is calculated. The measured time is the total time for a valid user to update the RL and recalculate the decryption key

dk_j and the PK. All these steps are done for the two cases. Figure 2 shows the timing results of the proposed scheme.

From figure 2, the time for keys recomputation differs according to the number of revoked users (R). As R increases, the total time for computation decreases. For instance, when $R = 30$, the computation time $T = 0.6$ Sec. in the first case and $T = 3.9$ Sec. in the second case. When $R = 120$, the computation time $T = 0.32$ Sec. in the first case, and $T = 1.85$ Sec. in the second case. The computation time in the second case is higher than that in the first case due to increasing the complexity with increasing the length of the security parameters r and q in the elliptic curve. For $R = 30$, $T = \{0.6, 3.9\}$ Sec. in the 1^{st}-case and the 2^{nd}-case respectively, and for $R = 120$, $T = \{0.32, 1.85\}$ Sec. in the 1^{st}-case and the 2^{nd}-case respectively. This result is consistent with the theoretical analysis in which the computation cost is $O(n - R)$.

The proposed scheme doesn't really need a long time for keys re-computation in any of the two cases because updating keys in the proposed RIBBE scheme doesn't need multi-level multi linear mapping, but only needs a simple exponentiation and multiplication.

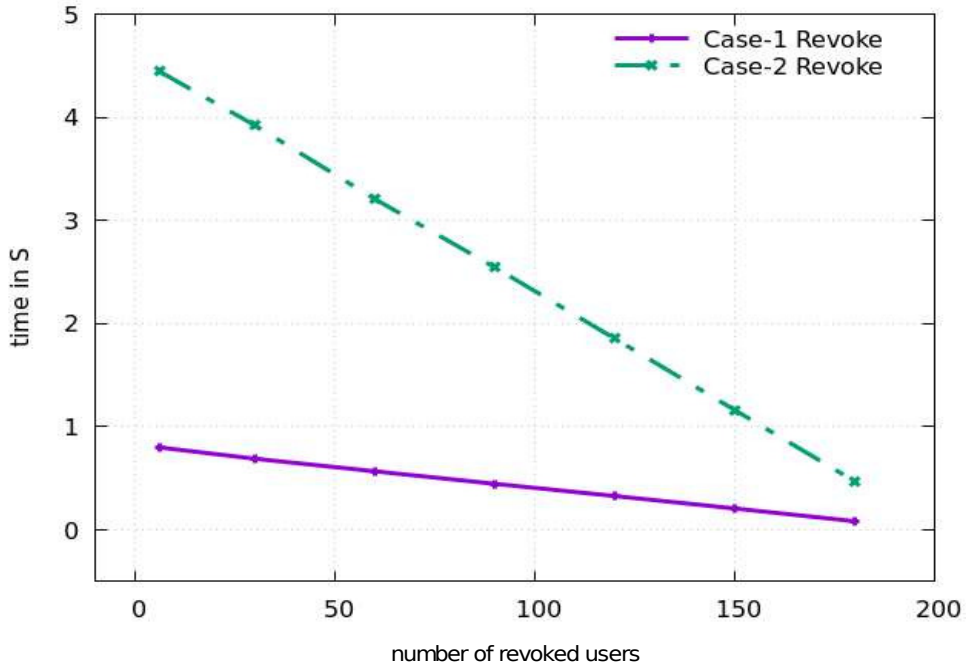

FIGURE 2. Simulation Results

7. **Security Analysis.** When trusted authority sends an element r_u at time τ to allow authorized users to update their parameters, each user has to update the RL and recalculate the decryption and public keys. The unauthorized or corrupted users won't be able to update their parameters and will be revoked permanently. So, the proposed scheme achieves a very crucial feature of broadcast encryption, which is forward and backward secrecy. Any revoked user won't be able to decrypt any new transmitted ciphertext which comply with the forward secrecy. Also, if a new user joined the network, then he won't be able to decrypt any of the old ciphertext as he doesn't have the old keys and that comply with the backward secrecy.

8. **Conclusions.** In this paper, an efficient scheme for identity based broadcast encryption (IBBE), and an efficient revocable identity-based broadcast encryption (RIBBE) scheme have been proposed. The proposed schemes are based on multi-linear pairing.

The proposed IBBE scheme allows a trusted authority (TA) to gather a number of users in a group, where any one of the users can broadcast an encrypted message to any subset of the group. Also, the proposed RIBBE scheme allows TA to revoke any user permanently. In IBBE, both of TA and users take apart in system setup, and new users can be added easily to the network. In RIBBE, both of TA and valid users participate in updating the system keys to allow revoking the unauthorized users permanently. The proposed schemes have employed two techniques already used in broadcast encryption schemes which are aggregatability and identity-based. The adoption of these techniques have achieved most of the required objectives in any broadcast encryption scheme as follows:

1. A fully Collusion Resistant scheme with Forward and Backward secrecy are achieved.
2. The scheme has a very acceptable computation cost in setup $\mathcal{O}(n)$.
3. The scheme can add users dynamically with computation and transmission cost $\mathcal{O}(n)$.
4. Temporary and Permanent Revocation with computation cost $\mathcal{O}(n - R)$.
5. A short overhead messages, and the message is transmitted only once for valid users.

The two proposed schemes have been implemented using the open source library Pairing-Based Cryptography (PBC)[14]. The execution time of the algorithms for each scheme has been computed to show that the theoretical analysis is consistent with the experimental analysis.

REFERENCES

[1] C.Gentry, "Certificate-based encryption and the certificate revocation problem", International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp.272–293, 2003.

[2] G. Erceylan and M. A. Akcayol, "Trust-Chain-Based Certificate Revocation Control in Autonomous Vehicle Networks," 2022 5th International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2022, pp. 42-47.

[3] A.Shamir , "Identity-based cryptosystems and signature schemes", Workshop on the theory and application of cryptographic techniques", Springer, pp.47–53, 1984

[4] S.Berkovits, "How to broadcast a secret", Workshop on the Theory and Application of Cryptographic Techniques, pp.535–541, 1991

[5] A.Fiat, and M.Naor, "Broadcast encryption", in Annual International Cryptology Conference, Springer, pp.480–491, 1993

[6] N.Kogan, Y.Shavitt, and A.Wool, "A practical revocation scheme for broadcast encryption using smart cards", ACM Transactions on Information and System Security (TISSEC), vol.9, pp.325–351, 2006.

[7] P. Sharma and B. R. Purushothama, "Analysis of Traditional Secure Group Key Management Schemes in Secure Multi-group Communication," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020.

[8] K. Lee and J. S. Kim, "A Generic Approach to Build Revocable Hierarchical Identity-Based Encryption," in IEEE Access, vol. 10, pp. 44178-44199, 2022.

[9] M.Naor, B.Pinkas, "Efficient trace and revoke schemes", Financial Cryptography: 4th International Conference, FC 2000 Anguilla, British West Indies, vol.4, pp.1–20, 2001

[10] A.Boldyreva, V.Goyal, and V.Kumar, "Identity-based encryption with efficient revocation", ACM conference on Computer and communications security, pp.417-426, 2008.

[11] A.Sahai, and B.Waters, "Fuzzy identity-based encryption", Advances in Cryptology–EUROCRYPT 2005, pp.457-473, 2005.

[12] H. Dahshan, H. M. Eldeeb, A. R. Shehata, "An Efficient Cryptographic-based Access Control Mechanism for Cloud Storage", Journal of Information Hiding and Multimedia Signal Processing, Vol. 15, No. 3, pp. 144-155, September 2024.

[13] Z. Guo, G. Wang, Y. Li, J. Ni and G. Zhang, "Attribute-Based Data Sharing Scheme Using Blockchain for 6G-Enabled VANETs", in IEEE Transactions on Mobile Computing, vol. 23, no. 4, pp. 3343-3360, April 2024.

[14] B. Lynn, "On the implementation of pairing-based cryptosystems", Ph. D. dissertation, Stanford University Stanford, California, 2007.

[15] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farr‘as, and J. A. Manjon, ”Contributory broadcast encryption with efficient encryption and short ciphertexts”, IEEE Transactions on Computers, vol. 65, no. 2, p 466–479, 2015.

[16] S.Park, K.Lee, and DH.Lee, ”New constructions of revocable identity-based encryption from multilinear maps”, IEEE Transactions on Information Forensics and Security, pp.1564–1577, 2015.

[17] M. Li, X. Xu, R. Zhuang, C. Guo, and X. Tan, “Identity-based broadcast encryption schemes for open networks”, in 2015 Ninth International Conference on Frontier of Computer Science and Technology, p 104–109, IEEE, 2015.

[18] D. Boneh, and M. K. Franklin, ”Identity-based encryption from the weil pairing”, In Joe Kilian, editor, CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer, 2001.

[19] A. Boldyreva, V. Goyal, and V. Kumar, ”Identity-based encryption with efficient revocation”, In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[20] Benoˆıt Libert, and Damien Vergnaud, ”Adaptive-id secure revocable identity-based encryption”, In Marc Fischlin, editor, CT-RSA 2009, volume 5473 of Lecture Notes in Computer Science, pages 1–15. Springer, 2009.

[21] J. H.Seo, and K. Emura, ”Revocable identity-based encryption revisited: Security model and construction”, In Kaoru Kurosawa and Goichiro Hanaoka, editors, PKC 2013, volume 7778 of Lecture Notes in Computer Science, pages 216–234. Springer, 2013.

[22] K. Lee, D. H. Lee, and J. H. Park, ”Efficient revocable identity-based encryption via subset difference methods”, Cryptology ePrint Archive, Report 2014/132, 2014. http://eprint. iacr.org/2014/132.