Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 4788031, 13 pages
https://doi.org/10.1155/2022/4788031

Research Article

An Efficient and Secure Data Sharing Method Using Asymmetric Pairing with Shorter Ciphertext to Enable Rapid Learning in Healthcare

Snehlata Yadav and Namita Tiwari

Department of Computer Science and Engineering, Maulana Azad National Institute of Technology, Bhopal 462003, India

Correspondence should be addressed to Snehlata Yadav; yadavsnehlata@gmail.com

Received 26 December 2021; Revised 27 January 2022; Accepted 3 February 2022; Published 20 April 2022

Academic Editor: Vijay Kumar

The recent advent of cloud computing provides a flexible way to effectively share data among multiple users. Cloud computing and cryptographic primitives are changing the way of healthcare unprecedentedly by providing real-time data sharing cost-effectively. Sharing various data items from different users to multiple sets of legitimate subscribers in the cloud environment is a challenging issue. The online electronic healthcare system requires multiple data items to be shared by different users for various purposes. In the present scenario, COVID-19 data is sensitive and must be encrypted to ensure data privacy. Secure sharing of such information is crucial. The standard broadcast encryption system is inefficient for this purpose. *Multichannel broadcast encryption* is a mechanism that enables secure sharing of different messages to different set of users efficiently. We propose an efficient and secure data sharing method with shorter ciphertext in public key setting using asymmetric (Type-III) pairings. The Type-III setting is the most efficient form among all pairing types regarding operations required and security. The semantic security of this method is proven under decisional BDHE complexity assumption without random oracle model.

1. Introduction

Cloud computing is a new paradigm of computing system that has revolutionized many sectors of Government and corporate such as academic, healthcare, online social networking, banking, and automobile. To enhance productivity, all these sectors consider data sharing as a vital tool to overcome the time and location constraints of resource usage such as computing power or data storage according to the need of users. Cloud computing environment provides large storage capacity and strong computation power. Thus, it brings ultimate convenience to the legitimate users. The outstanding advantage of cloud computing is that cloud service users can use their computing resources as a service with minimal cost at any time through the Internet that transcends geographical limits. Software as a Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) and Data-as-a-Service (DaaS) [1] are the four major services offered by cloud. Different cloud models support different services. There are many advantages in cloud, one of which is virtualization. Virtualization is also one of the strong pillars of cloud computing. Cloud computing system helps multiple users across the world to share and exchange their data in secure manner. Data sharing service is regarded as the most exciting use-case of cloud storage system, which has become the most important area in cloud computing. Apple's iCloud, Microsoft's Azure [2], and Amazon's S3 [3] are renowned for offering a more flexible and easy way to share data over the Internet. Despite this, they are susceptible to various security threats, which are the primary concerns of cloud users [2]. Security threats from external adversary are a bit obvious. However, nowadays, data owners outsource their data in the cloud server and want to share these data securely with other legitimate cloud users; various cryptography techniques can be adopted to enhance the secure exchange of data among subscribed users.

1.1. Problem Formulation. Consider an online e-healthcare system (Figure 1) where the data of patients such as COVID-19 data and OPD data from various data owners (doctors from several hospitals) are collected and uploaded to the centralized storage server, say cloud server, in encrypted form for security perspective, using a key, given by some authority such as hospital consortium. This is an example of data in transit. If this issue is not taken into consideration, the patients may suffer from enormous consequence of information leak. Recently millions of user data have been compromised. As per Government guidelines, there is a necessity to keep COVID-19 data private and secure.

In addition to COVID-19 and OPD data of patients, online healthcare system consists of doctors data, healthcare workers data, hospital data, pharmaceutical data, and so forth. Such crucial data uploaded in encrypted form are supposed to be analyzed and used by different legitimate data users; for example, due to this pandemic, a doctor could use information of patients to provide treatment and follow-up remotely, and a researcher/scientist at the research center could analyze patients record to find new symptoms appearing in patients. Based on their observation, they come up with the solutions and prevention methods. A business intelligence professional (BIF) could analyze patients records to generate the visualization of periodic health analysis report. A patient could search for a doctor (specialist) of their interest for better healthcare. An insurance company could use hospital data and pharmaceutical data for mediclaim disbursement and so forth. To accomplish all these tasks, the encrypted data stored on the server must be shared in efficient and flexible manner. However, an online healthcare system consists of multiple disjoint entities for data generation and data access. Since online healthcare data most of the time resides in shared environments, ensuring sharing and accessing the data securely on the cloud is a nontrivial task. One way to share data among a group of legitimate subscribers is broadcast encryption. Transmitting data to many groups of subscribers needs multiple instances of broadcast encryption which is highly inefficient. Multichannel broadcast encryption (Figure 2) is the efficient solution for sharing multiple data among multiple groups of legitimate subscribers in the cloud environment.

For example, we assume that our system model has 4 databases ($m = 4$): COVID-19 patient data, OPD patient data, doctors' data, and hospital data. The maximum number of subscribers for each database is 50 ($n = 50$). Assume that Alice (User1) is doctor, Bob (User2) is a researcher or scientist, Kim (User3) is a BI professional, and Ram (User4) is an officer from Insurance Company. If Dr. Alice is required to share COVID-19 patient data and OPD patient data, she subscribes to databases 1 and 2 and receives the corresponding decryption keys by hospital consortium. Bob wants to access COVID-19 data; he subscribes to database 1. Kim requires COVID-19 patient data, OPD patient data, doctors' data, and hospital data for making dashboards; she subscribes to databases 1, 2, 3, and 4. Ram requires doctors' data and hospital data for mediclaim and so forth; he subscribes to databases 3 and 4. The broadcaster encrypts data for the subscribers Alice, Bob, Kim, and Ram, using public parameters provided by hospital consortium. The broadcaster creates four target sets as follows:

(i) Set S_1 corresponding to database 1 (COVID-19 patient data), which is intended for Alice (User1), Bob (User2), and Kim (User3). The session key would be K_1. The legitimate subscribers are given as $S_1 = \{\text{User1,User2,User3}\}$.

(ii) Set S_2 corresponding to database 1 (OPD patient data), which is intended for Alice (User1) and Kim (User3). The session key would be K_2. The legitimate subscribers are given as $S_2 = \{\text{User1,User3}\}$.

(iii) Set S_3 corresponding to database 1 (doctors' data), which is intended for Kim (User3) and Ram (User4). The session key would be K_3. The legitimate subscribers are given as $S_3 = \{\text{User3, User4}\}$.

(iv) Set S_4 corresponding to database 1 (hospitals data), which is intended for Kim (User3) and Ram (User4). The session key would be K_4. The legitimate subscribers are given as $S_4 = \{\text{User3,User4}\}$.

In the above example, we have four subsets S_1, S_2, S_3, S_4. Thus, here targeted set of subscribers $t = 4$, where $t \leq m$. The detailed mathematical description of the scheme is presented in Section 3.

Another scenario could be an online academic system where online exam papers are distributed by some central authority. Let us take an example of Language paper; suppose that central authority of exam has to take 28 language papers corresponding to various states. The authority wants to send these exam question papers to authorised exam centers in a secure way. Multichannel broadcast encryption provides an efficient way for solving this problem. There are many real-time cases where multichannel broadcast encryption can be applied.

In this paper, we propose an efficient method of data sharing by multiple different users to multiple different legitimate subscribers in a secure and flexible way. The major contribution is listed as follows:

(i) Multichannel broadcast encryption scheme [4] is based on the setting of symmetric pairings. Type-I setting is slower as compared to Type-III setting [6]. The proposed scheme is constructed in Type-III setting. It is of interest to convert MCBE construction from symmetric to asymmetric bilinear pairings [5]. The asymmetric variant is definitely faster and efficient and has compact implementation, which will arise from the benefit over the symmetric setting.

(ii) Most of the schemes available in literature are in private key setting but the proposed scheme is in public key setting and has a small ciphertext size.

(iii) The semantic security of the scheme is based on Decisional Bilinear Diffie-Hellman Exponent (DBDHE) hardness assumption.

(iv) The proposed construction achieves selective security in the random oracle model (ROM).

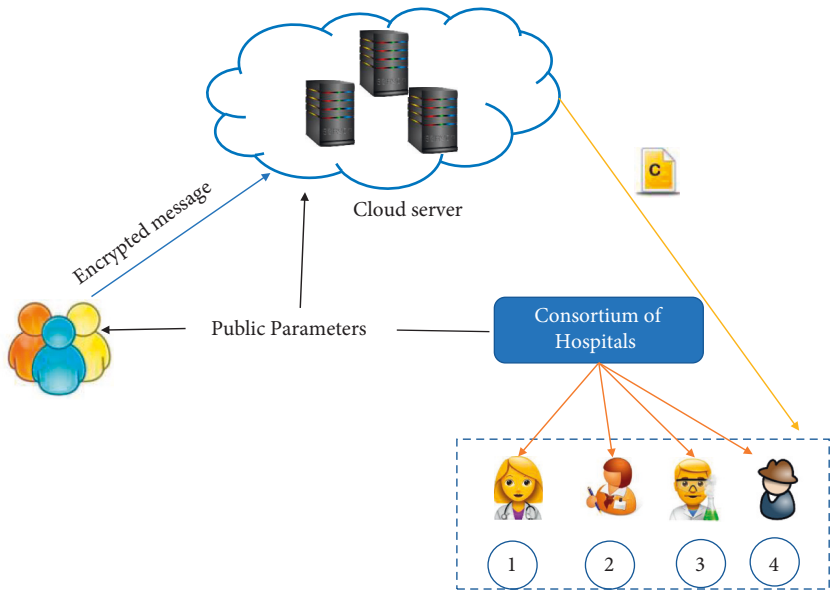

Figure 1: A system model for the e-healthcare scenario.

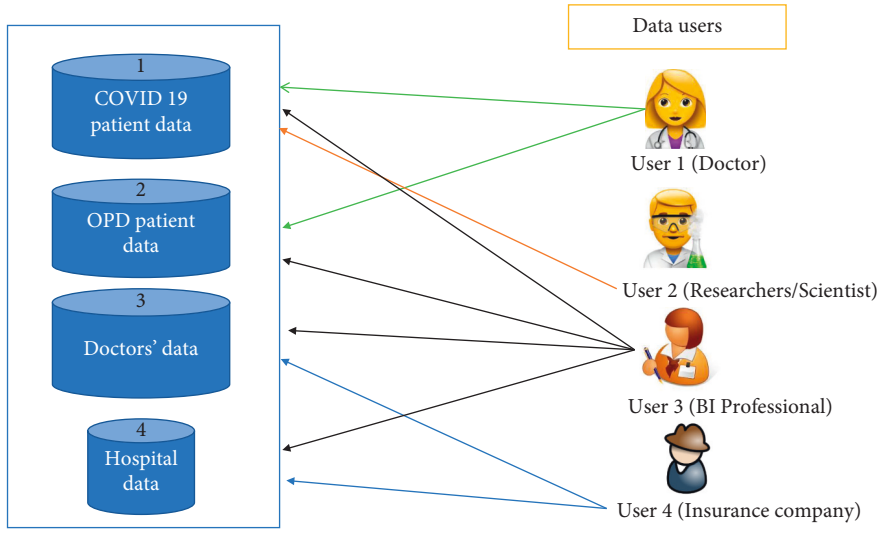

Figure 2: A MCBE-based system model for online data sharing.

The rest of the manuscript is organized as follows: Section 2 covers mathematical notations and computational complexity assumptions on which broadcast encryption schemes are constructed. The framework of conversion from symmetric setting to asymmetric setting is described in Section 3. In Section 4, the security model and correctness proof of conversion to asymmetric pairing are covered. The proposed scheme is then analyzed based on scheme complexity in Section 5. Section 6 concludes the paper including some open problems.

1.2. Related Work. Broadcast encryption [6] is a useful cryptographic primitive and has been widely studied as it is the fundamental primitive for many real-life applications. It was introduced by the seminal work of Fiat and Naor in year 1993, but it received much attention after the realization of Naor, Naor, and Lotspiech scheme [7]. Broadcast encryption cryptographic primitive provides a solution to the problem of communicating an encrypted message to only set S of legitimate users over insecure public channel. In more detail, users who get access to ciphertext are called privileged subscribers. They are members of set S and nonmembers of S are called revoked users. Thus, the broadcast algorithm is considered to work on the partition of revoked and legitimate users and the partition may vary for each broadcast message. Revoked users cannot learn a single bit of encrypted message even if they collude in some way. This property is called collusion resistance property. Due to this, broadcast encryption (BE) [8] has potential applications in fields such as pay TV, satellite TV, encrypted mailing services, and encrypted file system in cloud applications.

Broadcast encryption is deployed in two ways based on keys, namely, symmetric-key setting and asymmetric-key setting. In symmetric-key setting, a key generation center distributes the secret decryption key to all legitimate users in advance even before the message is transmitted. In such a scenario, only broadcaster acts as an emitter of message. The plaintext is encrypted by the emitter using a session key and in turn the session key is encrypted using the keys of the legitimate users of set S. So, for every new broadcast message, if new user joins and existing user leaves the system, the secret key has to be refreshed. Modifying and refreshing key, when at least one user leaves or joins in the system, is called one-affects-all problem. The problem is efficiently addressed by the broadcast encryption in public-key (asymmetric-key) setting. In this kind of setting, all users of S have a pair of keys: encryption key and decryption key. Broadcaster and other entities can act as emitter; however, only legitimate subscribers can decrypt the message and read the actual plaintext. It also alleviates the problem of refreshing the secret keys when a new member joins the system. The secure transmission of secret keys to all users of system has a problem of key compromise by members of S. Broadcast encryption is put forth by the seminal work of Fiat and Naor [6] followed by many constructions that have been proposed in [9] with different objectives of reducing decryption key size, encryption key size, encrypted message size, and computational cost of construction. Broadcast encryption in public-key setting is well studied and further categorized in Figure 3 as follows: identity-based broadcast encryption, attribute-based broadcast encryption, anonymous broadcast encryption, hierarchical broadcast encryption, dynamic broadcast encryption, and distributed broadcast encryption. Thus, it has many practical applications such as secure e-mail system, digital rights management system, pay TV, database security system, online social network system, and blockchain. Waters and Sahai [10] realized an extension of identity-based encryption which was later named as attribute-based encryption, in which inspite of identity as a public key, attributes of legitimate recipients are used for encrypting messages. ABE constructions' major problem is collusion resistance and recipient revocation. In some circumstances, one may want to give access right to a subset of recipients rather than only one specific recipient; to facilitate this, the notion of attribute-based broadcast encryption [11] has been realized. Figure 3 represents the broad categorization of broadcast encryption variants of it in public key framework.

(1) Identity-based broadcast encryption: the notion of identity-based broadcast encryption (IBBE) scheme was first introduced by Delerablée [12]. It is an extension of identity-based encryption scheme in public-key setting where, instead of public keys of the legitimate users, their identity, such as an e-mail id, passport number, and driving license number (strings of characters, alphanumeric values, and numerals), was used as encryption key to encode the message. IBBE is a practical cryptographic primitive that allows exponential number of recipients to exchange messages in secure manner; this implies that the public parameters are not correlated to decryption key of recipients and to ciphertext transmitted among subscribers. The first optimal IBBE scheme [13] has been constructed from pairings and learning with errors (LWE).

(2) Attribute-based broadcast encryption: Sahai and Waters [10] realized an extension of fuzzy identity-based encryption which was later termed as attribute-based encryption. In this, despite identity being a public key, attributes of legitimate recipients have been taken into account for encrypting messages which can be decrypted by a set S of subscribers, that is, those who belong to attribute set. ABE schemes suffer from the problem of collusion resistance and recipient revocation. Some scenario requires to provide access right to a subset of recipients rather than only one specific recipient. To facilitate this, the notion of attribute-based broadcast encryption [11] has been realized. ABBE has been well studied by the research community in recent years [14] which includes various hardness assumptions such as bilinear map, multilinear map, LWE, and R-LWE. LWE and R-LWE constructions are quantum-resistant but are not good candidates for resource-constrained environment as key size and ciphertext size become large for light weight devices [14].

(3) Anonymous broadcast encryption: in the standard broadcast encryption (BE) cryptosystem, recipients' information is revealed from the encrypted message. This is also considered as a security gap since it enables automatic disclosure of identity. However, many BE scenarios demand to hide the target identity, as the identity also conveys sensitive information and can cause identity threat, if it gets disclosed. The notion of anonymous BE gets rid of this and enables users to search on encrypted data. In year 2006, Barth et al. [15] introduced another variant of broadcast encryption (BE), known as *anonymous broadcast encryption* (Ano-BE) which is chosen-ciphertext-attack- (CCA-) secure in random oracle model (ROM). Subsequently, [16–18] have shown enhancement on this primitive.

(4) Dynamic broadcast encryption: in SCN 2012, Phan et al. [19] first introduced a primitive of BE called dynamic decentralized BE (D-BE). In the traditional broadcast encryption system, a central authority was responsible for management of a set of subscribers. To decentralize such a system, D-BE primitive uses subset cover framework with DDH hardness assumption.

(5) Hierarchical broadcast encryption: this variant of BE is constructed on pairing based cryptographic primitive that enables key delegation property to subsequent descendants in the hierarchical system.

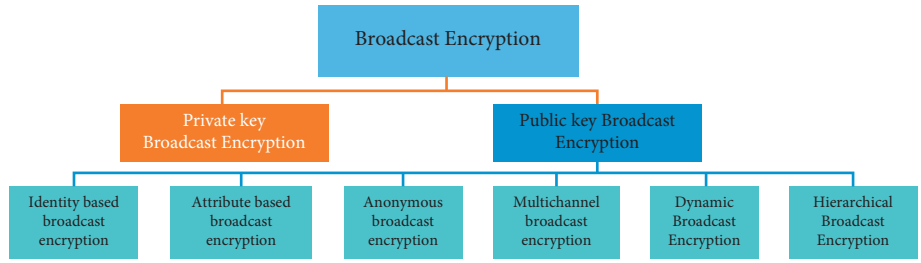

Figure 3: Categorization of broadcast encryption schemes.

This was first proposed by [20] for identity-based BE scheme. The later scheme is IND-CCA secure with constant ciphertext size in standard model.

(6) Functional broadcast encryption: this variant of BE enables access control along with public-key cryptography for sending encrypted file to specific subset of subscriber [21]. This scheme is based on indistinguishability obfuscation and achieves selective IND-CCA security.

(7) Multichannel broadcast encryption: this variant of BE enables sending an encrypted message to different groups of users. Consider a scenario of secret space program where the scientists of various states of a country are working together and the project coordinator wants to transmit different kinds of encrypted data to the various teams located in different geographical locations simultaneously. Multichannel broadcast encryption scheme was first presented by [4] in *ASIA CCS 13*. The scheme was designed in symmetric-key setting and achieves chosen-plaintext (CPA) and chosen-ciphertext security in standard model. It was further modified by [22]. In CANS 2018, [16] designed the scheme in public-key framework using decisional BDHE-sum assumption. The scheme has constant header size and achieves selective security. Acharya's [23] one construction achieves semistatic security and another construction achieves selective security with high computation cost. Both schemes are constructed in Type-I pairing [5]. Very recently, Le et al. [24] have constructed a scheme using GDDHE hardness assumption in public-key setting. The scheme achieves selective security in random oracle model.

Cloud is the most promising platform to share health related data. Online e-healthcare models [25, 26] are deploying cloud for sensitive data sharing. Many broadcast encryption primitives [27, 28] have been used for data sharing in cloud environment. These primitives are available in private- as well as public-key setting [29]. As far as our problem is concerned, we are interested in multichannel broadcast cryptographic primitives that allow sharing of different messages to different users. Most of the constructions are in private-key setting and Type-I pairing. However, these schemes suffer from the limitations of private-key settings as well as Type-I pairing setting.

2. Preliminaries

2.1. Notations. We introduce same notations as presented in [4]. The notations are summarized in Table 1. For a set B, let $b \xleftarrow{R} B$ indicate that b is a uniformly selected random element from set B. In the following, we will assume that there exists an asymmetric bilinear map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, where $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$ are groups of the elliptic curve of the same prime order q with generators P and Q, respectively. As both groups are of prime order, any non-identity elements of $\mathbb{G}_1$ and $\mathbb{G}_2$ are the generators of the group. Finally, any element in group $\mathbb{G}_1$, $\mathbb{G}_2$, or $\mathbb{G}_T$ is assumed to have size $\mathcal{O}(\eta_1), \mathcal{O}(\eta_2), \mathcal{O}(\eta_T)$, respectively.

Let α be a uniformly chosen random element of $\mathbb{Z}_q$. For any element N from either $\mathbb{G}_1$ or $\mathbb{G}_2$, let $N_x = \alpha^x N$, where $x \in \mathbb{Z}_q$.

Consider $\overrightarrow{Y}_{N,\alpha,l} = \{N_1, N_2, \ldots, N_l, N_{l+2}, \ldots, N_{2l}\}$ as a set of $2l-1$ elements. The term N_{l+1} is not included in $\overrightarrow{Y}_{N,\alpha,l}$, so that the bilinear pairing would be of a little help in evaluating $\hat{e}(P,Q)^{\alpha^{l+1}}$.

2.2. Bilinear Map Based on Prime Order Groups. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two additive groups of same prime order and let $\mathbb{G}_T$ be multiplicative cyclic group of prime order q for some large prime q. P is a generator of $\mathbb{G}_1$ and Q is a generator of $\mathbb{G}_2$; pairing is defined as a function $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ [30].

A pairing is defined to be admissible if it satisfies the following properties:

(1) Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab} = \hat{e}(bP, aQ)$, $\forall P \in \mathbb{G}_1$, $\forall Q \in \mathbb{G}_2$, and $\forall a, b \in \mathbb{Z}_q$.

(2) Nondegeneracy: $\hat{e}(P,Q)$ is a generator element of $\mathbb{G}_T$; that is, $\mathbb{G}_T = \langle \hat{e}(P,Q) \rangle$, where $\hat{e}(P,Q) \neq 1$.

(3) Computability: a pairing is defined as computable if there exists an algorithm that can compute $\hat{e}(P,Q)$, $\forall P \in \mathbb{G}_1, \forall Q \in \mathbb{G}_2$, and $\forall a, b \in \mathbb{Z}_q$ efficiently. There are three types of bilinear maps [31, 32] used in the construction of various pairing-based schemes:

(i) If $\mathbb{G}_1 = \mathbb{G}_2$, the pairing is termed as *symmetric pairing* or *Type-I* pairing

(ii) If $\mathbb{G}_1 \neq \mathbb{G}_2$ and there exists an efficiently computable homomorphism ϕ: $\mathbb{G}_2 \longrightarrow \mathbb{G}_1$, the pairing is referred to as *Type-II* pairing

(iii) If $\mathbb{G}_1 \neq \mathbb{G}_2$ and there does not exist an efficiently computable homomorphism ϕ: $\mathbb{G}_2 \longrightarrow \mathbb{G}_1$, the

Table 1: Notations.

Notation	Description
λ	Security parameter
Param	Public parameter
$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$	Cyclic groups
P, Q	Generator element
$\overrightarrow{Y}_{N,\alpha,l}$	Vector set
MSK	Master secret key
$\widehat{e}$	Pairing function
PK	Public key
SK	Decryption key
$\mathscr{C}, \mathscr{A}$	Algorithms

pairing is referred to as *asymmetric pairing* or *Type-III* pairing

2.3. Computational Complexity Assumption. In this section, the computational complexity assumption of multichannel broadcast encryption scheme is introduced. The symmetric and asymmetric versions of decisional BDHE assumption are proposed [28, 33].

2.3.1. Bilinear Diffie–Hellman Exponent (BDHE) Assumption in the Symmetric Pairing Setting. Let P and Q be two random generators of cyclic group $\mathbb{G}$ of prime order q and $\alpha \xleftarrow{[R]} \mathbb{Z}_p$ such that $Q_i = Q^{\alpha^i}$. The n-BDHE problem in $\mathbb{G}$ is defined as follows:

Let $\overrightarrow{Y}_{Q,\alpha,n} = (Q_1, \ldots, Q_n, Q_{n+2}, \ldots, Q_{2n})$
Input instance: $(P, Q, \overrightarrow{Y}_{Q,\alpha,n}, D)$
Output: $D = \widehat{e}(Q_{n+1}, P) = \widehat{e}(P, Q)^{\alpha^{n+1}} \in \mathbb{G}_T$

An algorithm $\mathscr{A}$ has advantage ϵ in solving n-BDHE problem in $\mathbb{G}$ if $\Pr[\mathscr{A}(P, Q, Q_1, \ldots, Q_n, Q_{n+2}, \ldots, Q_{2n}) = D] \geq \epsilon$, where the probability is over the random choices of generator $(P, Q) \in \mathbb{G}$, random choice of $\alpha \in \mathbb{Z}_p$, the random choice of $D \in \mathbb{G}_T$, and the random bits $\beta \in \{0, 1\}$ used by $\mathscr{A}$.

Definition 1. The decisional (τ, ϵ, l)-BDHE hardness assumption holds in $\mathbb{G}$ if no τ-time algorithm has advantage at least ϵ in solving the l–BDHE problem in $\mathbb{G}$ [33].

2.3.2. Bilinear Diffie–Hellman Exponent (BDHE) Assumption in the Asymmetric Pairing Setting. Security of multichannel broadcast encryption schemes in asymmetric bilinear pairing is based on the well-studied complexity assumption known as Bilinear Diffie-Hellman Exponent (BDHE) assumption [33]. Consider two bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of same prime order q. Given P, Q, and $\alpha^i P = P^{\alpha^i}$ in either $\mathbb{G}_1$ or $\mathbb{G}_2$, for $i = (1, 2, \ldots, l, l+2, \ldots, 2l)$, $\overrightarrow{Y}_{P,\alpha,l} = (P_1, P_2, \ldots, P_l, P_{l+2}, \ldots, P_{2l})$.

The asymmetric decisional l–BDHE problem is defined as follows.

Input instance: $(\mathscr{H}, P, Q, \overrightarrow{Y}_{P,\alpha,l}, \overrightarrow{Y}_{Q,\alpha,l}, D)$.
Output: $D = \widehat{e}(P_{l+1}, \mathscr{H}) \in \mathbb{G}_T$.

Since the term $l+1$ is missing from the sequence of powers, the bilinear map appears to be of no help in computation of $\widehat{e}(P_{l+1}, \mathscr{H})$. The bilinear pairing $\widehat{e}$ decides whether $D = \widehat{e}(P_{l+1}, \mathscr{H})$ holds or not. As a shorthand, once P, Q, and α are specified, y_i is set as $y_i = \alpha^i y = y^{\alpha^i}$, where y is in either $\mathbb{G}_1$ or $\mathbb{G}_2$.

Let *Adversarial* algorithm $\mathscr{A}$ be a τ-time algorithm that receives an input challenge for asymmetric l–BDHE problem and produces a decision bit $\beta \in \{0, 1\}$ as output. $\mathscr{A}$ has advantage ϵ in solving asymmetric decisional l–BDHE problem when the difference between $|\Pr[\mathscr{A}(\mathscr{H}, P, Q, \overrightarrow{Y}_{P,\alpha,l}, \widehat{e}(P_{l+1}, \mathscr{H})) = 0]|$ and $|\Pr[\mathscr{A}(P, Q, \overrightarrow{Y}_{P,\alpha,l}, \widehat{e}(P_{l+1}, \mathscr{H}) = 0)]|$ is $\geq \epsilon$, where the probability is over the random choices of $D \in \mathbb{G}_T$, random bits consumed by $\mathscr{A}$, random choice of $\alpha \in \mathbb{Z}_q$, and the random choices of generators P and Q of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

Definition 2. The asymmetric decisional (τ, ϵ, l)-BDHE hardness assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no τ-time algorithm has advantage at least ϵ in solving the asymmetric l–BDHE problem in $(\mathbb{G}_1, \mathbb{G}_2)$ [28].

2.4. Multichannel Broadcast Encryption. Multichannel broadcast encryption (MCBE) is a variant of broadcast encryption introduced by [4] inspired by the construction of [34]. In this cryptosystem, a Private-Key Generation Centre (PKGC) generates decryption keys and global public parameters. A broadcaster generates ciphertexts $\{C_i\}_{i=1}^m$ corresponding to a message M for m disjoint groups of legitimate users $\{G_i\}_{i=1}^m$. A legitimate user $u \in G_i$ retrieves the plaintext M using own decryption key. The description of MCBE cryptographic primitive scheme is as follows.

2.4.1. Syntax of MCBE. An MCBE scheme is four-tuple of algorithms: MCBE = (Setup, KeyGen, Enc, Dec).

(1) (Param, MSK)←Setup(N, λ): *Setup* is also known as PKGC which takes as input maximum count of users N accumulated in the system and security parameter λ. The PKGC outputs the public parameter Param and a master secret key MSK. Param is made public for all and MSK is kept secret.

(2) d_u←KeyGen(Param, MSK, u): it takes Param, MSK, and a legitimate user u as inputs and produces a decryption key d_u corresponding to user u as output. d_u is sent to u over a secure communication link established between PKGC and the legitimate user u.

(3) $(\mathscr{C}, \{K_i\}_{i=1}^m)$←Enc$(S_1, S_2, \ldots, S_m,$ Param): it takes input Param and set of legitimate users $\{S_i\}_{i=1}^m$, with each $S_i \subseteq G_i$. The broadcaster entity outputs a session key (K_i) for each group S_i and a ciphertext $\mathscr{C}$ for all groups. The broadcaster entity makes ciphertext $\mathscr{C}$ available publicly and session keys $(K_i)_{i=1}^m$ are kept secret in the system. To recover a ciphertext C_i for plaintext message M, one must have session key K_i. This scheme is based on symmetric-key encryption algorithm. If $S_i = \phi$ (null set) then the broadcaster entity sets $K_i = \perp$.

(4) $K_i \leftarrow \mathrm{Dec}(\mathrm{Param}, d_u, \mathscr{C}, \{S_i\}_{i=1}^{m})$: a subscribed user $u \in S_i$ retrieves his/her session key K_i corresponding to group S_i using d_u, Param, $\mathscr{C}$ and $(S_1, S_2, \ldots, S_m)$.

Correctness-The MCBE scheme holds correctly if, for a legitimate user $u \subseteq S_i$, the session key K_i can be fetched from ciphertext $\mathscr{C}$ correctly.

3. Conversion from Type-I Pairing to Type-III Pairing

Many novel applications have been constructed using pairing-based cryptographic protocols that are based on bilinear pairing map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_t$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are candidate prime order groups of a meticulously chosen elliptic curve $\mathscr{E}$ over a finite field $\mathbb{F}_q$, and $\mathbb{G}_t$ is a subgroup of finite field $\mathbb{F}_q$. Bilinear pairing is realizable from Weil, Tate, and other optimal pairings of elliptic curves [31].

Bilinear maps are studied extensively and have been efficiently implemented in past decades [35]. Bilinear pairings are broadly categorized into the following:

(1) Asymmetric pairing

(2) Symmetric pairing

(3) Composite order pairing

An *asymmetric pairing* is a general bilinear map that efficiently computes $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_t$, where $\mathbb{G}_1$ is a q-prime order group of points of an elliptic curve over a finite field $\mathbb{F}_q$ and $\mathbb{G}_2$ is also of the same prime order group of that elliptic curve over an extension field of $\mathbb{F}_q$. When the domains of bilinear map $\hat{e}$ are identical, such a pairing function $\hat{e}$ is referred to as a *symmetric pairing*. The third type of pairing is *composite order pairing* [36], where $\mathbb{G}_1$ is of composite order. The provision of additional flexibility makes computation of composite pairing slower. Waters' dual encryption system [37] was first constructed using composite order groups and in his later work composite order identity-based encryption is transformed and constructed using prime order bilinear pairing in asymmetric setting. The conversion from composite order bilinear pairing to prime order bilinear pairing was due to efficiency consideration. Studies have recommended that asymmetric pairings are faster and compact from the implementation viewpoint. Asymmetric bilinear pairings have the possibility to reduce the size of group in ciphertext and keys (public key and private key). There have been enormous cryptographic constructions realized on bilinear maps $\hat{e}: \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$. Here, multichannel broadcast encryption (MCBE) cryptographic primitive is built from bilinear pairings. Asymmetric bilinear pairings are further categorized into Type-II and Type-III bilinear pairings. In case of Type-II setting, there exists an efficiently computable isomorphism from group $\mathbb{G}_1$ to group $\mathbb{G}_2$ or vice versa, whereas in the Type-III pairing no such kind of isomorphism is known. Previous work has shown that the Type-III setting is the most efficient (among all pairing types) form in terms of operations required and security.

The following steps show the conversion from Type-I MCBE to Type-III MCBE for all the four algorithms (Setup, KeyGen, Enc, Dec).

(1) **Setup** $(1^\lambda, n)$:

(a) Randomly select $\alpha \in \mathbb{Z}_q$.
(b) Given $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle Q \rangle$.
(c) Select n random scalars $(x_1, x_2, \ldots, x_n)$.
(d) Evaluate $X_1 = Q^{x_1}, X_2 = Q^{x_2}, \ldots, X_n = Q^{x_n}$.
(e) Set Param $= (P, Q, \overrightarrow{Y}_{P,\alpha,n}, \overrightarrow{Y}_{Q,\alpha,n}, (X_1, X_2, \ldots, X_n))$.

(2) **Keygen** (MSK, PK)**:**

(a) Randomly select $\gamma \in \mathbb{Z}_q$ and set MSK $= (\gamma, \alpha, (x_1, x_2, \ldots, x_n))$.
(b) Set $v = P^\gamma \in \mathbb{G}_1$.
(c) Set public key PK $=$ (Param, $\gamma P, \gamma Q$).
(d) Secret key SK for users $i = 1, 2, \ldots, n$ is computed as $d_i = v^{\alpha^i}$.

(3) **Encrypt**
$(S_1, S_2, \ldots, S_m, \mathrm{Param}) \longrightarrow (\mathscr{C}, K_1, K_2, \ldots, K_m)$:

(a) Select a random scalar $r \xleftarrow{[R]} \mathbb{Z}_q$.
(b) Set $K_k = \hat{e}(P_n, Q_1)^{(r+\sum_{j \in S_k} x_j)}$.
(c) Evaluate

$$\mathscr{C}_1 = Q^r,$$

$$\mathscr{C}_2 = \prod_{k=1}^{m} \left(v \cdot \prod_{j \in S_k} P_{n+1-j} \right)^{\left(r + \sum_{j \in S_k} x_j \right)}. \tag{1}$$

(d) Set $\mathscr{C} = (\mathscr{C}_1, \mathscr{C}_2)$.
(e) Communicate $\mathscr{C}$.

(4) **Decrypt** $(S_1, S_2, \ldots, S_m, \mathscr{C}, d_i, i) \longrightarrow K_k$: if $i \in S_k$ then compute

$$K_k = \frac{\hat{e}(Q_i, \mathscr{C}_2)}{\hat{e}\left(d_i \cdot \prod_{j \neq i, j \in S_k} P_{n+1-j+i}, \mathscr{C}_1 \cdot \prod_{j \in S_k} X_j\right)} \cdot \frac{1}{\hat{e}\left(d_i \cdot \prod_{j \in S_l} P_{n+1-j+i}, \mathscr{C}_1 \cdot \prod_{j \in S_l} X_j\right)}. \tag{2}$$

Substituting the value of $\mathscr{C}_1$

$$
\begin{aligned}
&= \frac{\widehat{e}(Q_i, \mathscr{C}_2)}{\widehat{e}\left(d_i \cdot \prod_{j\neq i, j\in S_k} P_{n+1-j+i}\right), Q^r \cdot \prod_{j\in S_k} X_j} \cdot \frac{1}{\prod_{l=1 l\neq k} \widehat{e}\left(d_i \cdot \prod_{j\neq i, j\in S_k} P_{n+1-j+i}, Q^r \cdot \prod_{j\in S_k} X_j\right)} \\
&= \frac{\widehat{e}\left(Q^{\alpha^i}, \prod_{l=1}^{m} \left(\nu \cdot \prod_{j\in S_l} P_{n+1-j}\right)^{\left(r+\sum_{j\in S_l} x_j\right)}\right)}{\widehat{e}\left(\nu^{\alpha^i} \cdot \left(\prod_{j\neq i, j\in S_k} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_l} x_j\right)}\right)} \cdot \frac{1}{\prod_{l=1, l\neq k}^{l=m} \widehat{e}\left(\nu^{\alpha^i} \cdot \prod_{j\in S_l} P_{n+1-j+i}, Q^{\left(r+\sum_{j\in S_l} x_j\right)}\right)} \\
&= \frac{\widehat{e}\left(Q^{\alpha^i}, \nu \cdot \prod_{j\in S_l} P_{n+1-j+i}\right)^{\left(r+\sum_{j\in S_k} x_j\right)}}{\widehat{e}\left(\left(\nu \cdot \prod_{j\neq i, j\in S_k} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_k} x_j\right)}\right)} \cdot \prod_{l=1, l=k}^{m} \frac{\widehat{e}\left(Q^{\alpha^i}, \nu \cdot \prod_{j\in S_l} P_{n+1-j+i}\right)^{\left(r+\sum_{j\in S_l} x_j\right)}}{\widehat{e}\left(\left(\nu \cdot \prod_{j\neq i, j\in S_l} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_l} x_j\right)}\right)} \\
&= \frac{\widehat{e}\left(\left(\nu \cdot \prod_{j\in S_k} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_k} x_j\right)}\right)}{\widehat{e}\left(\left(\nu \cdot \prod_{j\neq i, j\in S_k} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_k} x_j\right)}\right)} \cdot \prod_{l=1, l=k}^{m} \frac{\widehat{e}\left(\alpha^i Q, \nu \cdot \prod_{j\in S_l} P_{n+1-j+i}\right)^{\left(r+\sum_{j\in S_l} x_j\right)}}{\widehat{e}\left(\left(\nu \cdot \prod_{j\neq i, j\in S_k} P_{n+1-j+i}\right)^{\alpha^i}, Q^{\left(r+\sum_{j\in S_l} x_j\right)}\right)} \\
&= \widehat{e}\left(P_{n+1-i}^{\alpha^i}, Q^{\left(r+\sum_{j\in S_k} x_j\right)}\right) \\
&= \widehat{e}\left(P_{n+1}, Q^{\left(r+\sum_{j\in S_k} x_j\right)}\right) \\
K_k &= \widehat{e}(P_n, Q_1)^{\left(r+\sum_{j\in S_k} x_j\right)}.
\end{aligned} \tag{3}
$$

4. Security Model

We also define the formal framework of security of MCBE scheme in asymmetric-pairing setting by the following game between the *adversarial algorithm* $\mathscr{A}$ and a *simulator algorithm* $\mathscr{C}$ in a real or random setting [38], as shown in Figure 4.

(1) **Setup**: the simulator algorithm $\mathscr{C}$ runs the *Setup* algorithm and outputs Param, MSK, and encryption key (PK).

(2) **Query Phase-I**: $\mathscr{A}$ adaptively asks queries to $\mathscr{C}$ which is also known as a Challenger. For some i-th user u_i, where $i = (1, 2, \ldots, n)$, $\mathscr{C}$ sends the decryption keys to $\mathscr{A}$. In response to the encryption query, $\mathscr{C}$ evaluates $\mathrm{Enc}(S_1, S_2, \ldots, S_m, \mathrm{Param})$ to produce $(K_1, K_2, \ldots, K_m, \mathscr{C})$ as output.

(3) **Challenge**: at this stage, $\mathscr{A}$ forwards the challenge set $(S_1^*, S_2^*, \ldots, S_t^*)$, where each $S_i^* \subseteq \{1, 2, \ldots, n\}$ for $i = 1, 2, \ldots, t$, as well as a target set S_j^*, where $j \in \{1, 2, \ldots, t\}$, to $\mathscr{C}$. In response to this, $\mathscr{C}$ forwards $(K_1^*, K_2^*, \ldots, K_t^*, \mathscr{C}^*)$. Then, $\mathscr{C}$ selects random $\beta \xleftarrow{[R]} \{0, 1\}$. Depending on the value of β, $\mathscr{C}$ replies with the following response $\mathscr{R}$:

$$
\mathscr{R} = \begin{cases} K_j^* \text{ is real key}, \beta = 0 \\ K_j^* \text{ is random}, \beta = 1 \end{cases}. \tag{4}
$$

(4) **Query Phase-II**: $\mathscr{A}$ continuously asks queries similar to *Query Phase-I*.

(5) **Guess**: now, $\mathscr{A}$ eventually returns decision bit $\beta' \in \{0, 1\}$ for β.

$$
\mathbf{Adv}_{\mathrm{MCBE}}^{\mathscr{A}} = \Pr[1 \leftarrow \mathscr{A} | \beta = 1] - \Pr[1 \leftarrow \mathscr{A} | \beta = 0]. \tag{5}
$$

Theorem 1. *The MCBE scheme in asymmetric setting is selectively secure under DBDHE assumption if it holds in* $(\mathbb{G}_1, \mathbb{G}_2)$. *For maximum n number of legitimate users,* $\mathbf{Adv}(\tau, q) \leq 2 \times \mathbf{Adv}^{b\ dh\ e}(\tau', n)$, *for* $\tau' \leq \tau + (xn + nq)T_e$, *where* T_e *denotes time complexity for exponentiation computation and m represents maximum number of available channels in the system.*

Proof. Let us consider that there exists Probabilistic Polynomial Time (PPT) algorithm, $\mathscr{A}$, such that $\mathbf{Adv}_{\mathrm{MCBE}}^{\mathscr{A}, n} > 1/2 + \epsilon$ for an MCBE system. We build a simulator algorithm $\mathscr{C}$ that has advantage in solving the DBDHE problem in $(\mathbb{G}_1, \mathbb{G}_2)$. Algorithm $\mathscr{C}$ takes as input a challenge

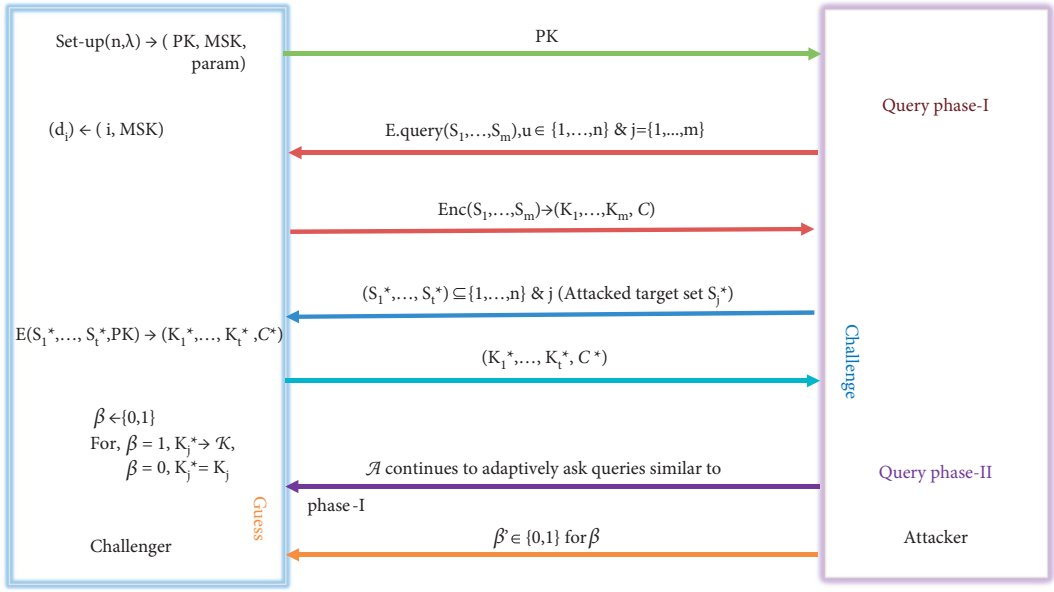

Figure 4: Security model of MCBE.

$(P, Q, \mathscr{H}, \overrightarrow{Y}_{P,\alpha,n}, \overrightarrow{Y}_{Q,\alpha,n}, D)$, where D is either $\hat{e}(P_{n+1}, \mathscr{H}) \in \mathbb{G}_T$ or a random element $\perp \in \mathbb{G}_T$. □

(1) Setup

(1) $\mathscr{C}$ generates global public parameters and secret keys d_i for $i \in S_k$. It selects a random scalar $r \in \mathbb{Z}_q$.

(2) Set $h = Q^r \Rightarrow h_i = Q_i^r$ for all $i = \{1, 2 \ldots, n\}$.

(3) Select random scalars $x_i \in \mathbb{Z}_q$ for $i = \{1, 2, \ldots, \eta, \ldots, n\}$ and compute $X_i = Q^{x_i}$.

(4) Choose a random index $\eta \in S_k$.

(5) $X_\eta = \mathscr{H} / \prod_{i \in S_k i \notin \eta} X_i = Q^{x_\eta}$. All scalars are known except x_η.

(6) $\mathscr{C}$ provides adversary the global public parameters: Param $= (P, Q, \overrightarrow{Y}_{P,\alpha,n}, \overrightarrow{Y}_{Q,\alpha,n}, \{X_i\}_{i=1}^n)$.

(7) $\mathscr{C}$ performs computation of secret decryption keys d_i except for $i \in S_k$.

(8) Select a random legitimate user $u \in \mathbb{Z}_q$ and define

$$\begin{aligned} \nu^{de\ f=} & \frac{Q^u}{\left(\prod_{j \in S_k} P_{n+1-j}\right)} \\ d_i^{de\ f=} & \frac{Q_i^u}{\left(\prod_{j \in S_k} P_{n+1-j+1}\right)} \\ = & \left(\frac{Q^u}{\prod_{j \in S_k} n + 1 - j}\right)^{\alpha^i}. \end{aligned} \tag{6}$$

Substituting the value of ν, we get

$$d_i = \nu^{\alpha^i} = \nu_i. \tag{7}$$

Moreover, since $d_i = \nu^{\alpha^i}$, it satisfies the specification parameters of the construction.

(2) Challenge

(1) Challenge C is simulator algorithm. while $\mathscr{C} = (\mathscr{C}_1, \mathscr{C}_2)$ is part of header, denotes cipher text both C and $\mathscr{C}$.

(2) $P_{j \in S_l} = \prod_{j \in S_l} P_{n+1-j}$ and $P_{j \in S_k} = \prod_{j \in S_k} P_{n+1-j}$. Evaluate $\mathscr{C}_2$ as

$$\mathscr{C}_2 = (h^u \cdot \mathscr{H}^u) + \prod_{l=1, l\neq k}^{m}\left(h^u \cdot \left(\frac{P_{j\in S_l}}{P_{j\in S_k}}\right)\cdot\left(\nu \cdot P_{j\in S_l}\right)^{\sum_{j\in S_l} x_j}\right)$$
$$(Q^u)^{r+\sum_{j\in S_k} x_j} + \prod_{l=1, l\neq k}^{m}\left(Q^{ru}\left(\frac{P_{j\in S_l}}{P_{j\in S_k}}\right)\cdot\left(\nu \cdot P_{j\in S_l}\right)^{\sum_{j\in S_l} x_j}\right) \tag{8}$$
$$= (Q^u)^{r+\sum_{j\in S_k} x_j} + \prod_{l=1, l\neq k}^{m}\left(\left(\frac{Q^u}{P_{j\in S_k}}\right)^r \cdot \left(P_{j\in S_l}\right)^r \cdot \left(\nu \cdot P_{j\in S_l}\right)^{\sum_{j\in S_l} x_j}\right).$$

Substituting the value of Q^u, we get

$$= \left(\nu P_{j\in S_k}\right)^{r+\sum_{j\in S_k} x_j} + \prod_{l=1, l\neq k}^{m}\left(\left(\frac{\nu P_{j\in S_k}}{P_{j\in S_k}}\right)^r \left(P_{j\in S_l}\right)^r \left(\nu P_{j\in S_l}\right)^{\sum_{j\in S_l} x_j}\right)$$
$$= \left(\nu \prod_{j\in S_k} P_{n+1-j}\right)^{r+\sum_{j\in S_k} x_j} + \prod_{l=1, l\neq k}^{m}\left(\nu \prod_{j\in S_l} P_{n+1-j}\right)^r \left(\nu \prod_{j\in S_l} P_{n+1-j}\right)^{\sum_{j\in S_l} x_j} \tag{9}$$
$$\prod_{l=1}^{m}\left(\nu \cdot \prod_{j\in S_l} P_{n+1-j}\right)^{r+\sum_{j\in S_l} x_j}.$$

The following notations were used: $P^r_{n+1-j} = h_{n+1-j}$ and $\mathscr{H} = Q^{\sum_{j\in S_i} x_j}$.

(3) Set $\mathscr{C} = (\mathscr{C}_1, \mathscr{C}_2)$.

(4) $D = \hat{e}(P_{n+1}, \mathscr{H})$ and $K_k = \hat{e}(Q_1, P_n)^{r+\sum_{j\in S_k} x_j}$.

(5) Thus, to generate session keys, $\mathscr{C}$ computes, for all $i \neq k$,

$$K_i = \hat{e}\left(P_{n+1}, Q\right)^{\sum_{j\in S_i} x_j} \cdot \hat{e}\left(P_{n+1}, Q^r\right) = \hat{e}\left(P_{n+1}, Q\right)^{r+\sum_{j\in S_i} x_j}, \tag{10}$$

and sets

$$K_k = D \cdot \hat{e}\left(P_{n+1}, Q^r\right). \tag{11}$$

(6) $\mathscr{C}$ produces the output $(\mathscr{C}, \{K_i\}_{i=1}^m)$ as a challenge to adversarial algorithm $\mathscr{A}$.

(7) If D is the correct value, then

$$K_k = \hat{e}\left(P_{n+1}, \mathscr{H}\right) \cdot \hat{e}\left(P_{n+1}, Q^r\right). \tag{12}$$

Substituting the value of $\mathscr{H}$, we get

$$K_k = \hat{e}\left(P_{n+1}, Q^{\sum_{j\in S_i} x_j}\right) \cdot \hat{e}\left(P_{n+1}, Q^r\right) \hat{e}\left(P_{n+1}, Q\right)^{r+\sum_{j\in S_i} x_j}. \tag{13}$$

If the value of element D is random, then K_k produces $\perp$ as output.

(3) Guess

$\mathscr{A}$ outputs a guess bit β' for β. $\mathscr{A}$ wins the game if $\beta' = \beta$. $\mathscr{C}$ produces the output $\mathscr{R}$:

$$\mathscr{R} = \begin{cases} 0, \beta' = \beta \\ 1, \beta' \neq \beta \end{cases}. \tag{14}$$

$\mathscr{R} = 0$ represents $D = \hat{e}(P_{n+1}, \mathscr{H})$; otherwise, when $\mathscr{R} = 1$, $D = \perp$.

$\mathscr{A}$'s advantage in breaking the security of the MCBE in asymmetric setting is defined in terms of the fact that the probability of occurrence of the event that $\beta' = \beta$ in the mentioned game is evaluated as $\mathbf{Adv}^{\mathscr{A}}_{MCBE} = |\Pr[\beta' = \beta] - 1/2|$

5. Result and Analysis

We have presented multichannel broadcast encryption (MCBE) scheme in asymmetric-pairing setting. The number of scalars, which have been used in the construction of MCBE (in symmetric-pairing setting), is analyzed. The following observations were made:

(1) Param uses scalars $(x_1, x_2, \ldots, x_n)$ and α. MSK uses scalars $(x_1, x_2, \ldots, x_n)$, α, and γ.

(2) Encrypt algorithm uses scalars r, γ, m (no. of groups).

Table 2: A comparative summary of various variants of MCBE schemes.

Parameters	[4]	[22]	[16]	[24]	[23]	Proposed
|Param|	$(3n-1)\|\mathbb{G}\|$	$(2n+m)\|\mathbb{G}\|$	$(2n+m+3)\|\mathbb{G}\|$	$(n+\text{mn}+1)\|\mathbb{G}_1\|$ $m\|\mathbb{G}_T\|$	$(3n+m+3)\|\mathbb{G}\|$	$(2n+m-1)\|\mathbb{G}_1\|$ $(2n-1)\|\mathbb{G}_{\mathbb{T}}\|$
|SK|	$1\|\mathbb{G}\|$	$1\|\mathbb{G}\|$	$1\|\mathbb{G}\|$	$1\|\mathbb{G}_1\|$	$2\|\mathbb{G}\|$	$1\|\mathbb{G}_1\|$
|CT|	$2\|\mathbb{G}\|$	$2\|\mathbb{G}\|$	$2\|\mathbb{G}\|$	$1\|\mathbb{G}_1\|$	$2\|\mathbb{G}\|$	$1\|\mathbb{G}_1\|$
Public key	No	No	Yes	Yes	Yes	Yes
Security	CPA	CPA	CPA	CPA	CPA	CPA
Hardness assumption	n-BDHE	n-BDHE	DBDHE-sum	GDDHE	n-BDHE	n-BDHE
Algebraic construction	Pairing based	Pairing based	Pairing based	Pairing based	Pairing based	Pairing based
Pairing type	Type-I	Type-I	Type-I	Type-III	Type-I	Type-III
Random oracle	No	No	No	Yes	No	No

Table 3: A comparison of various symmetric- and asymmetric-pairing-based MCBE schemes.

Schemes	# Param		# CT		# MSK		# SK		Pairing
	$\mathbb{G}_1$	$\mathbb{G}_T$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_1$	$\mathbb{Z}_q$	$\mathbb{G}_1$	$\mathbb{Z}_q$	
[4]	$3n-1$	–	2	–	2	$n+2$	2	$n+1$	SP
[22]	$2n+m$	–	2	–	2	–	1	2	SP
[16]	$2n+m+3$	–	2	–	2	n	1	2	SP
[24]	$n+mn+1$	m	1	1	1	$m+1$	1	m	AP
[23]	$3n+m+3$	–	2	–	2	–	2	–	SP
Proposed	$2n+m-1$	$2n-1$	1	1	–	$n+2$	1	2	AP

SP: symmetric pairing; AP: asymmetric pairing.

(3) Ciphertext uses r, γ scalars.

(4) Param, MSK, EK, and ciphertext consist of elements of group $\mathbb{G}_1$.

(5) $T = \hat{e}(P_{n+1}, G) \in \mathbb{G}_T$ [4].

Based on the above points, we have attempted a transformation of the scheme into Type-III pairing setting. The MCBE in asymmetric setting has the following points:

(1) Param uses $(2n-1)$ elements of $\mathbb{G}_1$ and $(3n-1)$ elements of $\mathbb{G}_2$. MSK uses scalars $(x_1, x_2, \ldots, x_n), \alpha$, and γ.

(2) Enc algorithm uses scalar r only.

(3) Ciphertext uses r and γ.

(4) Param and ciphertext consist of elements of groups $\mathbb{G}_1$ and $\mathbb{G}_2$.

(5) MSK and SK consist of elements of group $\mathbb{G}_2$.

(6) PK consists of elements of $(\mathbb{G}_1, \mathbb{G}_2)$.

(7) $D = \hat{e}(P_{n+1}, \mathcal{H}) \in \mathbb{G}_T$.

A comparison of features of MCBE scheme based on various complexity assumptions is shown in Table 2. The rows # Param, # PK, # SK, # CT, # EK, and # MSK represent the numbers of group elements in public parameter, public key, secret key, ciphertext, encryption key, and master secret key, respectively.

Group $\mathbb{G}_1$ consists of two parameters, Param and ciphertext. On the other hand, MSK and decryption keys (SK) are elements of $\mathbb{G}_2$. All MCBE schemes appearing in literature are included in Table 3.

Based on Tables 2 and 3, the following has been observed:

(i) The proposed scheme uses asymmetric pairings, whereas the rest of the schemes use asymmetric pairings. So, one could have $|\mathbb{G}_2| > |\mathbb{G}_1|$, which in turn leads to the smaller size ciphertext, reduced storage space, and enhanced performance [31].

(ii) As we have taken two group elements $\mathbb{G}_1$ and $\mathbb{G}_2$ and achieved compact size ciphertext which is the most important design consideration of broadcast encryption schemes, the public parameter size has increased in the proposed method. It is the limitation of this work. The public parameter is independent of the number of channels and users need to download it once. It does not increase any communication overhead.

6. Conclusion and Future Work

We have proposed an efficient and secure method for data sharing using asymmetric pairing (Type-III) with compact size ciphertext in public-key setting to enable rapid learning in healthcare environment. Our construction serves as an efficient solution for various practical data sharing applications such as healthcare environment, distribution of consumer product licence, and collaborative sharing to enable learning. Our construction is collusion-resistant and the security of the scheme is based on standard hardness assumption. We have demonstrated how this construction is modified to symmetric pairing to achieve compact size ciphertext. The analysis and result establish that the proposed scheme outperforms other existing schemes in terms of performance, storage, and transmission cost. The proposed

method offers the same level of security with reduced memory requirement. Reducing the size of public parameter as well as constructing the traitor tracing system for this scheme is left as open problem.

Data Availability

The data that support the findings of this study are available from the corresponding author upon request. The dataset is not required for this study.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] "Market and trends," https://blogs.idc.com/2021/04/19/the-data-as-a-service-market-in-2021-at-a-glance/.

[2] S. Sabitha and M. S. Rajasree, "Multi-level on-demand access control for flexible data sharing in cloud," *Cluster Computing*, vol. 24.

[3] "iCloud. (2014) Apple storage service," 2014, https://www.icloud.com/.

[4] D. H. Phan, D. Pointcheval, and V. C. Trinh, "Multi-channel broadcast encryption," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ASIA CCS '13*, pp. 277–286, ACM, Hangzhou China, May 2013.

[5] O. Uzunkol and M. S. Kiraz, "Still wrong use of pairings in cryptography," *Applied Mathematics and Computation*, vol. 333, pp. 467–479, 2018.

[6] A. Fiat and M. Naor, *Broadcast Encryption*, pp. 480–491, 1993.

[7] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology CRYPTO 2001*, J. Kilian, Ed., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 41–62, 2001.

[8] M. Ak, "Optimization techniques and new methods for broadcast encryption and traitor tracing," https://www.thesis.bilkent.edu.tr/0006211.pdf.

[9] K. Fukushima, S. Kiyomoto, T. Tanaka, and K. Sakurai, "Ternary subset difference method and its quantitative analysis," in *Information Security Applications*, K.-I. Chung, K. Sohn, and M. Yung, Eds., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 225–239, 2009.

[10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2005*, R. Cramer, Ed., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 457–473, 2005.

[11] D. Lubicz and T. Sirvent, "Attribute-based broadcast encryption scheme made efficient," in *Proceedings of the Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa*, pp. 325–342, Casablanca, Morocco, June 2008.

[12] C. Delerablée, "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*, pp. 200–215, Springer-Verlag, Kuching Malaysia, December 2007.

[13] S. Agrawal and S. Yamada, "Optimal broadcast encryption from pairings and LWE," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, A. Canteaut and Y. Ishai, Eds., Springer, Zagreb, Croatia, pp. 13–43, May 2020.

[14] T. V. X. Phuong, G. Yang, W. Susilo, and X. Chen, *Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key*, University of Wollongong Australia, Australia, pp. 252–269, 2015.

[15] A. Barth, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *Financial Cryptography and Data Security*, G. Di Crescenzo and A. Rubin, Eds., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 52–64, 2006.

[16] K. Acharya and R. Dutta, "Constructions of secure multi-channel broadcast encryption schemes in public key framework," in *Cryptology and Network Security*, J. Camenisch and P. Papadimitratos, Eds., Springer International Publishing, Cham, pp. 495–515, 2018.

[17] X. Li and R. Yanli, "Efficient anonymous identity-based broadcast encryption without random oracles," *International Journal of Digital Crime and Forensics*, vol. 6, no. 2, pp. 40–51, 2014.

[18] N. Fazio and I. M. Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts," in *Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, PKC'12*, pp. 225–242, Springer-Verlag, Darmstadt Germany, May 2012.

[19] D. H. Phan, D. Pointcheval, and M. Strefler, "Decentralized dynamic broadcast encryption," in *Security and Cryptography for Networks*, I. Visconti and R. De Prisco, Eds., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 166–183, 2012.

[20] W. Liu, J. Liu, Q. Wu, B. Qin, and Y. Li, "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption," *International Journal of Information Security*, vol. 15, no. 1, pp. 35–50, 2016.

[21] H. Wang, Y. Zhang, K. Chen, G. Sui, Y. Zhao, and X. Huang, "Functional broadcast encryption with applications to data sharing for cloud storage," *Information Sciences*, vol. 502, pp. 109–124, 2019, https://www.sciencedirect.com/science/article/pii/S0020025519305663.

[22] X. W. Zhao and H. Li, "Improvement on a multi-channel broadcast encryption scheme," *Applied Mechanics and Materials*, vol. 427-429, pp. 2163–2169, 2013.

[23] K. Acharya, "Secure and efficient public key multi-channel broadcast encryption schemes," *Journal of Information Security and Applications*, vol. 51, p. 102436, 2020.

[24] M. H. Le, V. D. Tran, V. A. Trinh, and V. C. Trinh, "Compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption," *Theoretical Computer Science*, vol. 804, pp. 219–235, 2020.

[25] T. Kanwal, A. Anjum, and A. Khan, "Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities," *Cluster Computing*, vol. 24, no. 1, pp. 293–317, 2021.

[26] M. L. Florence and D. Suresh, "Enhanced secure sharing of PHR's in cloud using user usage based attribute based encryption and signature with keyword search," *Cluster Computing*, vol. 22, no. S6, pp. 13119–13130, 2019.

[27] M. Mandal and K. Nuida, "Identity-based outsider anonymous broadcast encryption with simultaneous individual messaging," *Network and System Security*, pp. 167–186, 2020.

[28] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 891–904, 2017.

[29] S. Agrawal and S. Yamada, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12105 LNCS*, Springer, New York, US, pp. 13–43, 2020.
[30] "Elliptic curves , group law , and efficient computation," 2010.
[31] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008, https://www.sciencedirect.com/science/article/pii/S0166218X08000449.
[32] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, and L. Chen, "Report on pairing-based cryptography," *Journal of Research of the National Institute of Standards and Technology*, vol. 120, p. 11, 2015.
[33] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT'05*, pp. 440–456, Springer-Verlag, Aarhus Denmark, May 2005.
[34] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology - CRYPTO 2005*, V. Shoup, Ed., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 258–275, 2005.
[35] B. Lynn, *Ben Lynn June 2007 (June)*, pp. 1–126, 2007.
[36] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," *Theory of Cryptography*, vol. 3378, pp. 325–341, 2005.
[37] B. Waters, "Dual system encryption: realizing fully secure ibe and hibe under simple assumptions," in *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '09*, pp. 619–636, Springer-Verlag, Santa Barbara CA, August 2009.
[38] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proceedings of the 8th International Conference on Theory and Practice in Public Key Cryptography, PKC'05*, pp. 65–84, Springer-Verlag, Berlin, Heidelberg, 2005.