Hindawi
Security and Communication Networks
Volume 2018, Article ID 7202598, 13 pages
https://doi.org/10.1155/2018/7202598

Research Article

A Secure and Privacy-Aware Smart Health System with Secret Key Leakage Resilience

Yinghui Zhang,[1,2,3] **Pengzhen Lang**,[1] **Dong Zheng**,[1,2] **Menglei Yang**,[1] **and Rui Guo**[1]

[1]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[2]*Westone Cryptologic Research Center, Beijing 100070, China*
[3]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

Correspondence should be addressed to Yinghui Zhang; yhzhaang@163.com

Received 30 January 2018; Revised 16 April 2018; Accepted 30 May 2018; Published 24 June 2018

Academic Editor: Karl Andersson

With the development of the smart health (s-health), data security and patient privacy are becoming more and more important. However, some traditional cryptographic schemes can not guarantee data security and patient privacy under various forms of leakage attacks. To prevent the adversary from capturing the part of private keys by leakage attacks, we propose a secure leakage-resilient s-health system which realizes privacy protection and the safe transmission of medical information in the case of leakage attacks. The key technique is a promising public key cryptographic primitive called leakage-resilient anonymous Hierarchical Identity-Based Encryption. Our construction is proved to be secure against chosen plaintext attacks in the standard model under the Diffie-Hellman exponent assumption and decisional linear assumption. We also blind the public parameters and ciphertexts by using double exponent technique to achieve the recipient anonymity. Finally, the performance analysis shows the practicability of our scheme, and the leakage rate of the private key approximates to 1/6.

1. Introduction

With the development of information technology, the Internet of Things (IoT) has become a very important technology for government departments, businesses, and academic circles in various countries with its huge application scenes. The technology of IoT is based on the Internet to achieve the communication between information and terminal equipment, information, and real goods. At present, IoT has been widely used in many fields, like food safety, smart health (s-health), urban construction, cloud storage, etc. [1–4].

The cloud-based s-health systems play an important role in our daily life. At present, doctors use computers to store and retrieve patients' electronic health records (EHRs). EHRs systems replace paper systems and thus increase efficiency in the recording, storage, and retrieval of patients information [5–7]. However, EHRs which reveal highly confidential personal information stored in the cloud and exchanged over the Internet can be vulnerable to attack [8–10], such as data loss, hackers hijacking information, and integrity. In recent years, a large number of medical information leaks in cloud storage have attracted more and more people's attention. Data privacy and security is believed to be the major challenge in the deployment of EHR-based healthcare system. There has been a lot of work that deals with data privacy and security problems [11–15].

However, the traditional cryptographic schemes may not be secure under various forms of leakage attacks, such as side-channel attacks [16] and cold-boot attack [17]. Such attacks exploit various forms of information leakage by observing physical implementations of cryptosystems, such as running time [18], electromagnetic radiation [19], power consumption, and fault detection [20]. IoT generally adopts discrete network structure, and most of the nodes are located outdoors, which makes it easy for attackers to obtain sensitive information [21–23]. Therefore, it is very meaningful to construct a secure and privacy-aware smart health system with secret key leakage resilience in the case of leakage attacks. Based on the paper of Zhang et al. [24], we construct

a leakage-resilient anonymous HIBE scheme in s-health data sharing [25–27] scenarios.

1.1. Our Contributions. To address the medical information security and privacy of the patients issues in s-health, we propose a secure s-health system which allows a medical information owner to securely share data in the case of leakage attacks. The main contributions of this paper as follows.

(i) Firstly, we present the system model of a secure s-health system based on a leakage-resilient anonymous HIBE scheme. Our system addresses the problem of key management and reduces the pressure of PKG.

(ii) Secondly, we blind the public parameters and ciphertexts using double exponent technique to achieve the anonymity, so as to achieve the effect of protecting privacy.

(iii) Finally, our scheme is built in prime order groups that are more computationally efficient than composite order groups. The proposed scheme is proved to be secure against chosen plaintext attacks in the standard model.

1.2. Related Work. More attention to identity-based encryption (IBE) has been attracted since the notion of IBE was introduced by Shamir [28]. The private key for the user in traditional IBE schemes [29] is generated by the Private Key Generation Center (PKG). However, in a large scale network, such as s-health, the number of users is huge, and the task of PKG is too heavy and it is difficult to manage the user's private key. In order to solve this problem, the notion of Hierarchical Identity-Based Encryption (HIBE) was proposed [30] and then many HIBE schemes were proposed [31, 32]. What is more, many anonymous HIBE schemes were proposed [33–36] where the ciphertext does not leak the identity of the recipient. However, their sizes of private keys and ciphertexts increase with the depth of identity hierarchy. Zhang et al. [24] proposed an anonymous HIBE scheme over prime order groups where both private keys and ciphertext have a constant size.

Dillema et al. [37] proposed a simple cryptographic access control method in the prehospital environment. However, this system provides access privilege if and only if patient and health worker meet in the physical world. Zhang et al. [38] proposed a reference model of the security and privacy issues in the EHR cloud and requirements for secure access of EHR data. A secure EHR system demonstrated to be resilient to various attacks to protect patient privacy and enable emergency healthcare was proposed by Sun et al. [39]. In e-Health and Mobile Health network, Guo et al. [40, 41] proposed a privacy-preserving attribute-based authentication system, which leverages users verifiable attributes to authenticate users while preserving their privacy issues. Kumar et al. [42] proposed a biometric based authentication scheme which is lightweight and solely uses symmetric key based operations. A secure data sharing using IBE scheme for the implementation of data sharing in the e-Healthcare system was proposed by Sudarson et al. [43]. Zhang et al. [44] proposed a system architecture and adversary model of a secure s-health system which realizes fine-grained access control on s-health cloud data and hence ensures users privacy protection. Dawoud et al. [45] defined different scenarios for the integration of the e-health systems with the cloud computing systems and these scenarios discussed the authentication and data processing in the different parts of the system. Zhang et al. [46] proposed a three-factor authenticated key agreement scheme based on a dynamic authentication mechanism to protect the users privacy using for e-health systems, and it was proved to be semantically secure under the real or random model. Sahi et al. [47] reviewed the latest research with regard to privacy preservation in e-Healthcare and explored whether this research offers any possible solutions to patient privacy requirements for e-Healthcare. However, these schemes may not be secure under various forms of leakage attacks.

The first leakage-resilient cryptographic scheme was proposed by Dziembowski and Pietrzak [48] that can capture most of the key leakage attacks. However, they constructed the leakage-resilient encryption scheme based on "only computation leaks information" which can not capture the cold-boot attack. To resist the cold-boot attack, the bounded-leakage model [49] was proposed by Akavia et al. What is more, the relative-leakage model [50] was proposed by Naor et al. Leakage resilience (anonymous) IBE schemes have been discussed previously. A leakage-resilient IBE scheme was proposed and showed being secure in the standard model by Alwen et al. [51]. Chow et al. [52] proposed three new leakage-resilient IBE schemes under the respective static assumptions of the original systems. Li et al. [53] proposed a new leakage-resilient public key encryption and showed that it was secure under Decisional Diffie-Hellman (DDH) assumption. Liu et al. [54] showed that the techniques of dual system technique lead to leakage resilience and proposed an anonymous leakage-resilient identity-based encryption scheme. Li et al. [55] proposed a new leakage-resilient IBE scheme in the bounded-leakage model and showed being semantically secure against adaptive chosen ciphertext attack in the standard model.

1.3. Organization. Some preliminaries are reviewed in Section 2. In Section 3, we define the usage scenario for smart healthcare system and present the system model and leakage-resilient security model. The secure s-health system based on leakage-resilient anonymous HIBE is described in Section 4. In Section 5, our security analysis and leakage resilience analysis are described. Finally, we draw our conclusions in Section 6.

2. Preliminaries

2.1. Notations. For ease of reference, important notations are summarized in Table 1.

2.2. Random Extractor. We define the statistical distance between two random variables X and Y over a finite domain Ω to be

$$SD(X,Y) = \frac{1}{2}\sum_{w\in\Omega} |Pr[X = w] - Pr[Y = w]|. \quad (1)$$

Table 1: Notations used throughout the paper.

Notation	Description	Notation	Description	Notation	Description
SD	statistical distance	X, Y	random variable	Ω	finite domain
Pr	probability	$H_\infty(X)$	min-entropy	$\widetilde{H}_\infty(X \mid Y)$	average min-entropy
e	bilinear map	Ext	extractor	G, G_T	cyclic group
g	generator	$\mathcal{A}, \mathcal{B}$	algorithm	ε	advantage
PK	public key	MSK	master secret key	ID	identities
d_{ID}	private key	$L_{d_{ID}}$	number of leaked bits	D_{ID}	rerandomize private keys
$\ell(\lambda)$	leakage parameter	f	leakage function	$\perp$	reject symbol
M	message	CT	ciphertext	p	large prime number
v_{ij}	vector of Identity	h_{ij}	auxiliary parameters	s	random seed
l	maximum depth of HIBE	V	view without leakage	ρ	leakage ratio

The min-entropy of a random variable X is defined as

$$H_\infty(X) = -\log\left(\max_x Pr[X = x]\right). \tag{2}$$

The average min-entropy of a random variable X conditioned on another random variable Y is defined as follows:

$$\widetilde{H}_\infty(X \mid Y) = -\log\left(E_{y \leftarrow Y}\left[2^{-H_\infty(X|Y=y)}\right]\right). \tag{3}$$

Definition 1. If, for all pairs of random variables (X, Y) such that $X \in (0,1)^u$ and $\widetilde{H}_\infty(X \mid Y) \geq k$, it holds that

$$SD\left((Ext(X,S), S, Y), (U_m, S, Y)\right) \leq \varepsilon, \tag{4}$$

where S is uniform over $(0,1)^t$, we call polynomial-time function $Ext : (0,1)^u \times (0,1)^t \rightarrow (0,1)^m$ an average-case (k, ε)-strong extractor.

Lemma 2. *If* Y *has* 2^r *possible values and Z is random variable, we have*

$$\widetilde{H}_\infty(X \mid (Y, Z)) \geq \widetilde{H}_\infty(X \mid Z) - r. \tag{5}$$

2.3. Bilinear Groups. Let G and G_T be two cyclic groups of prime order p and $e : G \times G \rightarrow G_T$ be a bilinear map. We call G a bilinear group if it has the following properties:

(i) Bilinearity: $\forall u, v \in G$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

(ii) Nondegeneracy: for the generator $g \in G$, we have $e(g, g) \neq 1$.

(iii) Computability: $\forall u, v \in G$, the bilinear map $e(u, v)$ can be efficiently computed.

2.4. Computational Assumptions

2.4.1. Bilinear Diffie-Hellman Exponent (BDHE) Assumption. Let g be a generator of group G and $\alpha, c \in Z_p^*$. We define the computational $(n+1)$−BDHE problem [56] to be

$$\begin{aligned} &input : \left(g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2}\right) \in G, \\ &output : e\left(g, y_0\right)^{\alpha^{n+1}} \left(= e\left(g, g\right)^{\alpha^{n+1} c}\right), \end{aligned} \tag{6}$$

where $y_0 = g^c$, $y_i = g^{\alpha^i}$. Algorithm $\mathcal{A}$ has advantage ε in solving the computational $(n+1)$−BDHE problem if

$$\begin{aligned} &Pr\left(\mathcal{A}\left(g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2}\right)\right. \\ &\left. = e\left(g, y_0\right)^{\alpha^{n+1}}\right) \geq \varepsilon. \end{aligned} \tag{7}$$

The decisional version of the $(n+1)$−BDHE problem is defined in the usual manner.

$$\begin{aligned} &input : \left(g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2}, K\right), \\ &ouput : b \in \{0, 1\}. \end{aligned} \tag{8}$$

Let $K' = (g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2})$; Algorithm $\mathcal{B}$ has advantage ε in solving the decisional $(n+1)$−BDHE problem if

$$\begin{aligned} &Pr\left(\mathcal{B}\left(K', e\left(g, y_0\right)^{\alpha^{n+1}}\right) = 0\right) - Pr\left(\mathcal{B}\left(K', K\right) = 0\right) \\ &\geq \varepsilon. \end{aligned} \tag{9}$$

2.4.2. Decisional Linear Assumption. The decisional linear problem [57] is defined as

$$\begin{aligned} &input : \left(g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, K\right), \\ &ouput : b \in \{0, 1\}. \end{aligned} \tag{10}$$

Algorithm $\mathcal{A}'s$ goal is to output 1 when $K = g^{z_3 + z_4}$ or 0 otherwise. We give three weak versions of the decisional linear problem [35] as follows:

(i) Version (1):

$$\begin{aligned} &input : \\ &\left(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^{n+1}}, g^{z_2^n / z_1}, g^{z_2^{n+1} / z_3}, g^{z_4}, K\right), \\ &ouput : b \in \{0, 1\}. \end{aligned} \tag{11}$$

Algorithm $\mathcal{A}'s$ goal is to output 1 when $K = g^{z_1(z_3 + z_4)}$ or 0 otherwise.

(ii) Version (2):

$$input : \left(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n}, g^{z_2^{n+2}}, \ldots, g^{z_2^{2n}}, g^{z_3}, g^{z_4}, g^{z_4 z_2}, \ldots, g^{z_2^n z_4}, K\right), \quad (12)$$

$$ouput : b \in \{0, 1\}.$$

Algorithm $\mathscr{A}'s$ goal is to output 1 when $K = g^{z_1(z_3+z_4)}$ or 0 otherwise.

(iii) Version (3):

$$input : \left(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n}, g^{z_2^{n+2}}, g^{z_2^{2n}}, \ldots, g^{z_3}, g^{z_4}, g^{z_4 z_2}, \ldots, g^{z_2^n z_4}, g^{z_1 z_2}, \ldots, g^{z_2^n z_1}, K\right), \quad (13)$$

$$ouput : b \in \{0, 1\}.$$

Algorithm $\mathscr{A}'s$ goal is to output 1 when $K = g^{z_1(z_3+z_4)}$ or 0 otherwise.

3. System Model

3.1. Usage Scenario. The hospital uses the system software developed by our proposal, and each member of the hospital is registered in the system at a certain level. The system allocates private keys to them through the key generation algorithm; however, the private key generated may be leaked partly by malicious attackers through various forms of leakage attacks.

A patient, named Alice, visits a doctor in this hospital. According to condition, a nurse assigns Alice to the doctor named Bob. Through diagnosis, Bob thinks that Alice needs the doctor named Carol to treat the illness together. And Bob uploads Alice's EHRs to the cloud server with public key of Carol through the system. Carol uses his private key to download and decrypt Alice's EHRs. They complete the diagnosis and treatment of Alice.

During the entire process, Bob sends Alice's EHRs to Carol through the cloud, but Carol's private key may have leaked partly. If the general system is used, Alice's EHRs may be leaked, but our program can ensure that Alice's EHRs will not be leaked. Thus, the patient's EHRs have been protected safely.

3.2. System Model. We divide the system model into two parts, and the first part is shown in Figure 1, which is to produce the private keys to the different level of users (patients, doctors). The S-Health Authority (SHA) is an entity that produces the public key parameters and the master secret key. In our system, the level is divided into l levels. The private key of users in the first level is defined as the root private key. The private key of the k-th level users is related to the private key of the $(k-1)$-th level users, where $k \leq l$.

The second part is shown in Figure 2, which is to share medical information among all users. It is described in the picture where doctor A shares medical information to patient B. A encrypts medical information with B's public key

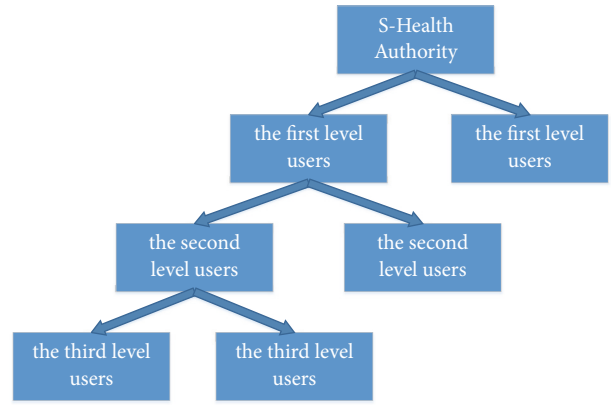

Figure 1: The generation of the private keys.

(identity) and then uploads it to the s-health cloud (SHC). Then B decrypts medical information with its own private key. The adversary $\mathscr{A}$ can know part of the private keys information of B through the leak attack.

We define an description of the proposed secure s-health system:

(i) Initialization: SHA produces the public key parameters PK and the master secret key MSK. All users can obtain PK.

(ii) User Registration: A user (a patient, a doctor) can join the s-health system by confirming its level to SHA.

(iii) Information Upload: A user encrypts medical information based on a leakage-resilient anonymous HIBE scheme and uploads the final ciphertext to SHC.

(iv) Information Access: A user downloads a ciphertext from SHC. The ciphertext can be decrypted if and only if the private keys correspond to the public key used for encryption.

3.3. Leakage-Resilient Security Model for Anonymous HIBE. The security of leakage-resilient anonymous HIBE is defined by the following game ($\boldsymbol{Game}_{\text{real}}$) between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$.

(i) Init: The adversary $\mathscr{A}$ gives the challenge identity ID^* to the challenger $\mathscr{C}$.

(ii) Setup: $\mathscr{C}$ computes $(PK, MSK) \leftarrow Setup(\lambda)$. $\mathscr{C}$ gives PK to $\mathscr{A}$ and keeps MSK to itself. $\mathscr{C}$ will initialize a set $S = \emptyset$, which will be the set of tuples of identities; private keys have been created and the number of leaked bits corresponds to the private key d_{ID} $(ID, d_{ID}, L_{d_{ID}})$. Let $\ell(\lambda)$ be a leakage parameter.

(iii) Phase 1: $\mathscr{A}$ adaptively issues the following two kinds of queries:

(a) Private Key Queries: $\mathscr{A}$ adaptively queries $\mathscr{C}$ with ID where $ID \neq ID^*$ and ID is not a prefix of ID^*; $\mathscr{C}$ responds with the private key d_{ID} corresponding to the identity ID.

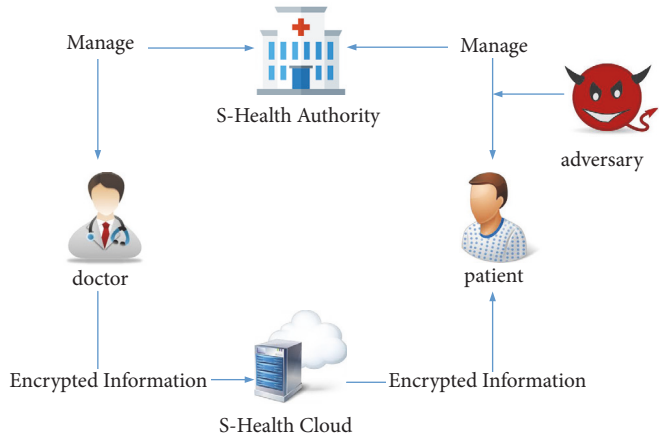

Figure 2: The sharing of medical information.

(b) Leak Queries: $\mathscr{A}$ gives a polynomial-time leakage function $f : \{0,1\} \to \{0,1\}$ and adaptively queries $\mathscr{C}$ with ID. $\mathscr{C}$ finds the tuple $(ID, d_{ID}, L_{d_{ID}})$ and replies with $f(d_{ID})$ when $L_{d_{ID}} + |f(d_{ID})| \leq \ell(\lambda)$ or a reject symbol $\perp$.

(iv) Challenge: $\mathscr{A}$ selects two messages M_0, M_1 on which it wishes to be challenged. $\mathscr{C}$ chooses a random bit $b \leftarrow \{0,1\}$ and gives $CT = Encrypt(params, ID^*, M_b)$ to $\mathscr{A}$.

(v) Phase 2: $\mathscr{C}$ answers the queries in the same way as phase 1 with the added restriction that $\mathscr{A}$ can not execute leakage queries.

(vi) Guess: $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$ and wins if $b' = b$.

Definition 3. We say that an anonymous HIBE scheme is leakage-resilient and selectively secure against chosen plaintext attacks (ANO-IND-sID-CPA) if all polynomial-time adversaries $\mathscr{A}$'s advantage is negligible in the above game. We define $\mathscr{A}$'s advantage to be

$$\boldsymbol{Adv}_{HIBE,\mathscr{A}}^{ANO-IND-sID-CPA} = \left| Pr\left[b = b'\right] - \frac{1}{2} \right|. \quad (14)$$

4. Secure s-Health System

4.1. A Leakage-Resilient Anonymous HIBE Scheme. For an HIBE of maximum depth l and an identity $ID_j = (v_1, \cdots, v_j)$ where $1 \leq j \leq l$, a leakage-resilient anonymous HIBE scheme is defined as follows:

(i) Setup$(\lambda) \to (PK, MSK)$: The Setup algorithm takes a security parameter λ and produces the public key parameters PK and the master secret key MSK. All users can obtain PK.

(ii) KenGen$(PK, ID_j, d_{ID|j-1}) \to d_{ID|j}$: The KenGen algorithm takes as input the public key PK, an identity $ID_j = (v_1, \ldots, v_j)$, and the private key $d_{ID|j-1}$ corresponding to the identity $(v_1, \ldots, v_{j-1})$. It outputs the private key $d_{ID|j}$.

(iii) Encrypt$(PK, ID_j, M) \to CT$: The Encrypt algorithm takes as input the public key PK, an identity $ID_j = (v_1, \ldots, v_j)$, and a message M. It outputs a ciphertext CT.

(iv) Decrypt$(PK, d_{ID|j}, CT) \to M$: The Decrypt algorithm takes as input the public key PK, a ciphertext CT, and the private key $d_{ID|j}$ corresponding to the identity $ID_j = (v_1, \ldots, v_j)$. It outputs the message M or a reject symbol $\perp$ if the ciphertext is invalid.

4.2. Description of Secure s-Health System. Let p be a large prime number and G be a group of order p. Let l be the HIBE of maximum depth and represent identity information as bit strings of length n [58].

(i) Initialization: SHA randomly chooses $\alpha, t_1, t_2, t_3 \in Z_p$. Set $v = g^{t_1}$, $g_1 = v^{\alpha}$, $u = g^{t_2}$, $x = g^{t_3}$, and then pick g_2, w in group G at random. The public key parameters are

$$PK = \{g, g_1, g_2, v, u, x, w\}. \quad (15)$$

The master secret key is $MSK = g_2^{\alpha}$.

(ii) User Registration: The user joins the s-health system and gets its private keys. The user initiates the following key generation protocol.

KeyGen: The KeyGen algorithm is defined as follows.

(a) Root private keys: For the first level user $ID_1 = (v_1)$ where $v_1 = (v_{11}, \ldots, v_{1n})$ and $v_{1i} \in \{0,1\}$, root PKG randomly chooses $\{\alpha_{11}, \ldots, \alpha_{1n}, \beta_{11}, \ldots, \beta_{1n}\} \in Z_p$ and produces the auxiliary parameters

$$h_{1i} = \left(h_{1(i-1)}\right)^{\alpha_{1i}^{v_{1i}} \beta_{1i}^{1-v_{1i}}}, \quad (16)$$

where $h_{10} = g$, $1 \leq i \leq n$, and h_{1n} is outputted as the public key. Root PKG outputs the private key for ID_1 as

$$d_{ID_1} = (d_{10}, d_{11}, d_{12}, d_{13}, d_{14}, d_{15}) = \left(g_2^{\alpha} h_{1n}^{r_1}, g^{r_1}, v^{r_1}, w^{r_1}, u^{r_1 t_1}, x^{r_1 t_1}\right) \quad (17)$$

and

$$D_{ID_1} = (D_{10}, D_{11}, D_{12}, D_{13}, D_{14}, D_{15}) = \left(h_{1n}^{r_2}, g^{r_2}, v^{r_2}, w^{r_2}, u^{r_2 t_1}, x^{r_2 t_1}\right), \quad (18)$$

where $r_1, r_2 \in Z_p$ and D_{ID_1} are used to rerandomize the private keys.

(b) Delegate: For the k-th level user $ID_k = (v_1, \ldots, v_k)$ where $k \le l$, $v_i = (v_{i1}, \ldots, v_{in})$ and $v_{ij} \in \{0, 1\}$, by using the private key $d_{ID|k-1}$ corresponding to the $(k-1)$-th level user $ID_{k-1} = (v_1, \ldots, v_{k-1})$:

$$d_{ID_{k-1}} = (d_{(k-1)0}, d_{(k-1)1}, d_{(k-1)2}, d_{(k-1)3}, d_{(k-1)4}, d_{(k-1)5}) = \left(g_2^{\alpha} \left(\prod_{i=1}^{k-1} h_{in}\right)^{r_1'}, g^{r_1'}, v^{r_1'}, w^{r_1'}, u^{r_1' t_1}, x^{r_1' t_1}\right) \quad (19)$$

and

$$D_{ID_{k-1}} = (D_{(k-1)0}, D_{(k-1)1}, D_{(k-1)2}, D_{(k-1)3}, D_{(k-1)4}, D_{(k-1)5}) = \left(\left(\prod_{i=1}^{k-1} h_{in}\right)^{r_2'}, g^{r_2'}, v^{r_2'}, w^{r_2'}, u^{r_2' t_1}, x^{r_2' t_1}\right). \quad (20)$$

PKG_k randomly chooses

$$\{\alpha_{k1}, \ldots, \alpha_{kn}, \beta_{k1}, \ldots, \beta_{kn}\} \in Z_p, \quad (21)$$

and it produces the auxiliary parameters

$$h_{kj}' = \left(h_{k(j-1)}'\right)^{\alpha_{kj}^{v_{kj}} \beta_{kj}^{1-v_{kj}}} = \left(g^{r_1'}\right)^{\prod_{j=1}^{n} \alpha_{kj}^{v_{kj}} \beta_{kj}^{1-v_{kj}}},$$
$$h_{kj}'' = \left(h_{k(j-1)}''\right)^{\alpha_{kj}^{v_{kj}} \beta_{kj}^{1-v_{kj}}} = \left(g^{r_2'}\right)^{\prod_{j=1}^{n} \alpha_{kj}^{v_{kj}} \beta_{kj}^{1-v_{kj}}}, \quad (22)$$

where $h_{k0}' = d_{(k-1)1}, h_{k0}'' = D_{(k-1)1}$ and $1 \le j \le n$.

Let $h_{kn} = g^{\prod_{j=1}^{n} \alpha_{kj}^{v_{kj}} \beta_{kj}^{1-v_{kj}}}$; then one can obtain $h_{kn}' = (h_{kn})^{r_1'}$ and $h_{kn}'' = (h_{kn})^{r_2'}$. PKG_k outputs the private key for ID_k as

$$d_{ID_k} = (d_{k0}, d_{k1}, d_{k2}, d_{k3}, d_{k4}, d_{k5}) = \left(d_{(k-1)0} \left(h_{kn}'\right)^{r'} \cdot \left(D_{(k-1)0} h_{kn}''\right)^{r'}, d_{(k-1)1} D_{(k-1)1}^{r'}, d_{(k-1)2} D_{(k-1)2}^{r'}, d_{(k-1)3} D_{(k-1)3}^{r'}, d_{(k-1)4} D_{(k-1)4}^{r'}, d_{(k-1)5} D_{(k-1)5}^{r'}\right) = \left(g_2^{\alpha} \left(\prod_{i=1}^{k} h_{in}\right)^{r_1}, g^{r_1}, v^{r_1}, w^{r_1}, u^{r_1 t_1}, x^{r_1 t_1}\right) \quad (23)$$

and

$$D_{ID_k} = (D_{k0}, D_{k1}, D_{k2}, D_{k3}, D_{k4}, D_{k5}) = \left(\left(D_{(k-1)0} h_{kn}''\right)^{r'}, D_{(k-1)1}^{r'}, D_{(k-1)2}^{r'}, D_{(k-1)3}^{r'}, D_{(k-1)4}^{r'}, D_{(k-1)5}^{r'}\right) = \left(\left(\prod_{i=1}^{k} h_{in}\right)^{r_2}, g^{r_2}, v^{r_2}, w^{r_2}, u^{r_2 t_1}, x^{r_2 t_1}\right), \quad (24)$$

where $r_1 = r_1' + r' r_2', r_2 = r' r_2', r' \in Z_p^*$.

(iii) Information Upload: A user encrypts medical information based on a leakage-resilient anonymous HIBE scheme as follows.

Encrypt: The encryptor randomly chooses $s_1, s_2 \in Z_p$ and a random seed $s \in \{0, 1\}^t$. The encryptor creates the ciphertext as follows:

$$CT = (C_0, C_1, C_2, C_3, C_4, C_5) = \left(M \oplus Ext\left(e(g_1, g_2)^{s_1}, s\right), \left(\prod_{i=1}^{k} h_{in}\right)^{s_1} \cdot u^{s_2}, w^{s_1} x^{s_2}, g^{s_2}, v^{s_1}, s\right). \quad (25)$$

(iv) Information Access: A user downloads and decrypts a ciphertext from SHC as follows.

Decrypt: The k-th level user decrypts a ciphertext CT using the private key $d_{ID|k}$ and computes

$$M = Ext\left(\frac{e(d_{k0}, C_4)\, e(d_{k4} d_{k5}, C_3)\, e(d_{k3}, C_4)}{e(C_1, d_{k2})\, e(C_2, d_{k2})}, C_5\right) \oplus C_0. \quad (26)$$

4.3. Correctness. The correctness can be checked:

$$\frac{e(d_{k0}, C_4)\, e(d_{k4} d_{k5}, C_3)\, e(d_{k3}, C_4)}{e(C_1, d_{k2})\, e(C_2, d_{k2})} = \frac{e\left(g_2^{\alpha} \left(\prod_{i=1}^{k} h_{in}\right)^{r_1}, v^{s_1}\right) e\left((ux)^{r_1 t_1}, g^{s_2}\right) e\left(w^{r_1}, v^{s_1}\right)}{e\left(\left(\prod_{i=1}^{k} h_{in}\right)^{s_1} u^{s_2}, v^{r_1}\right) e\left(w^{s_1} x^{s_2}, v^{r_1}\right)} = e(g_1, g_2)^{s_1}. \quad (27)$$

5. Analysis

5.1. Security Analysis. Following [59], the security proof can be completed by a series of hybrid games. Let $(C_0, C_1, C_2, C_3, C_4, C_5)$ denote the challenge ciphertext given to the adversary during a $\boldsymbol{Game}_{\text{real}}$. We define the hybrid games to be

(1) ***Game 1***: $C = (C_0, C_1, C_2, C_3, C_4, C_5)$;

(2) ***Game 2***: $C = (R_0, C_1, C_2, C_3, C_4, C_5)$;

(3) ***Game 3***: $C = (R_0, R_1, C_2, C_3, C_4, C_5)$;

(4) ***Game 4***: $C = (R_0, R_1, R_2, C_3, C_4, C_5)$,

where $R_0 \in G_T$ and $R_1, R_2 \in G$.

We will show these games are indistinguishable in the following lemmas.

Lemma 4. *Suppose the decision $(n+1)$-BDHE assumption holds, there is no polynomial-time adversary that can distinguish **Game 1** and **Game 2**.*

Proof. The proof follows from the security of the Boneh-Boyen selective-ID scheme [60] and Abdalla's security analysis [58]. Suppose there is adversary $\mathcal{A}$ that can distinguish between ***Game 1*** and ***Game 2*** with advantage ε. Then challenge $\mathcal{C}$ will be made to solve the decision $(n+1)$-BDHE assumption.

$\mathcal{C}$ receives a challenge tuple $(g, y_0, y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2}, K)$ where $y_0 = g^c$, $y_i = g^{\alpha^i}$, and K is either $e(g,g)^{\alpha^{n+1}c}$ or a random element of G_T. $\mathcal{C}$ interacts with $\mathcal{A}$ as follows:

(i) Init: The adversary $\mathcal{A}$ gives the challenge identity $ID^* = (v_1^*, \ldots, v_k^*)$ to the challenger $\mathcal{C}$ where $k \le l$.

(ii) Setup: $\mathcal{C}$ randomly chooses $t, t_1, t_2, t_3, \gamma, \alpha_{ij}, \beta_{ij} \in Z_p^*$, where $1 \le i \le l$, $1 \le j \le n$. It sets

$$\begin{aligned} v &= g^{t_1}, \\ g_1 &= y_1^{t_1}, \\ u &= g^{t_2}, \\ x &= g^{t_3}, \\ w &= g^t, \\ g_2 &= y_n g^\gamma. \end{aligned} \tag{28}$$

The public key parameters are $PK = \{g, g_1, g_2, v, u, x, w\}$. The master secret key is $MSK = g_2^\alpha = y_1^\gamma y_{n+1}$, which is unknown to $\mathcal{C}$.

(iii) Phase 1: $\mathcal{A}$ adaptively queries $\mathcal{C}$ with $ID = (v_1, \ldots, v_k)$ where $ID \ne ID^*$ and ID is not a prefix of ID^*. This condition ensures that there is $j \in \{1, \ldots, k\}$ such that $v_j \ne v_j^*$. $\mathcal{C}$ produces the private key corresponding to the identity $ID_j = (v_1, \ldots, v_j)$, where j denotes the first element such that $v_j \ne v_j^*$. Let τ be the number of sites such that $v_{ji} = v_{ji}^*$ in v_j. To respond to the query, $\mathcal{C}$ produces the auxiliary parameters as follows. For $1 \le i \le j$, compute

$$\begin{aligned} h_{i1} &= g^{\alpha_{i1}^{v_{i1}} \beta_{i1}^{1-v_{i1}}} \quad if\ v_{i1} \ne v_{i1}^*, \\ h_{i1} &= y_1^{\alpha_{i1}^{v_{i1}} \beta_{i1}^{1-v_{i1}}} \quad if\ v_{i1} = v_{i1}^*. \\ h_{i2} &= h_{i1}^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} \ne v_{i2}^*, \\ h_{i2} &= y_1^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} = v_{i2}^* \wedge v_{i1} \ne v_{i1}^*, \\ h_{i2} &= y_2^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} = v_{i2}^* \wedge v_{i1} = v_{i1}^*. \end{aligned} \tag{29}$$

Finally, the auxiliary parameters can be computed as follows.

$$\begin{aligned} h_{1n} &= y_n^{T(v_1)}, \\ &\cdots, \\ h_{(j-1)n} &= y_n^{T(v_{j-1})}, \\ h_{jn} &= y_\tau^{T(v_j)}, \end{aligned} \tag{30}$$

where $T(v_i) = \prod_{j=1}^n \alpha_{ij}^{v_{ij}} \beta_{ij}^{1-v_{ij}}$, for $1 \le i \le j, \tau \le n$. $\mathcal{C}$ randomly chooses $r_1' \in Z_p$ and sets $r_1 = r_1' - \alpha^{n-\tau+1}/T(v_j)$. The private keys corresponding to the identity ID_j are simulated as follows.

$$\begin{aligned} d_{j0} &= y_1^\gamma \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \left(y_\tau^{T(v_j)}\right)^{r_1'}, \\ d_{j1} &= g^{r_1'} y_{n-\tau+1}^{-1/T(v_j)}, \\ d_{j2} &= g^{r_1' t_1} y_{n-\tau+1}^{-t_1/T(v_j)}, \\ d_{j3} &= g^{r_1' t} y_{n-\tau+1}^{-t/T(v_j)}, \\ d_{j4} &= g^{r_1' t_1 t_2} y_{n-\tau+1}^{-t_1 t_2/T(v_j)}, \\ d_{j5} &= g^{r_1' t_1 t_3} y_{n-\tau+1}^{-t_1 t_3/T(v_j)}. \end{aligned} \tag{31}$$

In fact,

$$\begin{aligned} d_{j0} &= y_1^\gamma \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \left(y_\tau^{T(v_j)}\right)^{r_1'} \\ &= y_{n+1} y_1^\gamma \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_\tau^{T(v_j)}\right)^{r_1'} y_{n+1}^{-1} \\ &= g_2^\alpha \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_\tau^{T(v_j)}\right)^{r_1'} y_{n+1}^{-1} \\ &= g_2^\alpha \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_\tau^{T(v_j)}\right)^{r_1'} \left(y_\tau^{T(v_j)}\right)^{-\alpha^{n-\tau+1}/T(v_j)} \end{aligned}$$

$$= g_2^{\alpha}\left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'}\left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right)$$
$$\cdot\left(y_\tau^{T(v_j)}\right)^{(r_1'-\alpha^{n-\tau+1}/T(v_j))}$$
$$= g_2^{\alpha}\left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{(r_1'-\alpha^{n-\tau+1}/T(v_j))}$$
$$\times\left(y_\tau^{T(v_j)}\right)^{(r_1'-\alpha^{n-\tau+1}/T(v_j))}$$
$$= g_2^{\alpha}\left(\prod_{i=1}^{j} h_{in}\right)^{(r_1'-\alpha^{n-\tau+1}/T(v_j))} = g_2^{\alpha}\left(\prod_{i=1}^{j} h_{in}\right)^{r_1}. \tag{32}$$

In addition,

$$\begin{aligned} d_{j1} &= g^{r_1'} y_{n-\tau+1}^{-1/T(v_j)} = g^{r_1}, \\ d_{j2} &= g^{r_1' t_1} y_{n-\tau+1}^{-t_1/T(v_j)} = v^{r_1}, \\ d_{j3} &= g^{r_1' t} y_{n-\tau+1}^{-t/T(v_j)} = v^{r_1} = w^{r_1}, \\ d_{j4} &= g^{r_1' t_1 t_2} y_{n-\tau+1}^{-t_1 t_2/T(v_j)} = u^{r_1 t_1}, \\ d_{j5} &= g^{r_1' t_1 t_3} y_{n-\tau+1}^{-t_1 t_3/T(v_j)} = x^{r_1 t_1}. \end{aligned} \tag{33}$$

Then we can obtain

$$\begin{aligned} d_{ID_j} &= \left(d_{j0}, d_{j1}, d_{j2}, d_{j3}, d_{j4}, d_{j5}\right) \\ &= \left(g_2^{\alpha}\left(\prod_{i=1}^{j} h_{in}\right)^{r_1}, g^{r_1}, v^{r_1}, w^{r_1}, u^{r_1 t_1}, x^{r_1 t_1}\right). \end{aligned} \tag{34}$$

$\mathscr{C}$ also produces D_{ID_j}. $\mathscr{C}$ uses d_{ID_j} to derive a private key for the descendant identity ID_k and gives $\mathscr{A}$ the result.

Then, $\mathscr{A}$ submits the leak queries to $\mathscr{C}$.

(iv) Challenge: $\mathscr{A}$ selects two messages M_0, M_1 on which it wishes to be challenged. $\mathscr{C}$ first produces the auxiliary parameters as $h_{in} = g^{T_i^*}$ for challenge identity ID^*, where $T_i^* = T(v_i^*)$. $\mathscr{C}$ then randomly chooses $s_1, s_2 \in Z_p$ and a random seed $s \in \{0,1\}^t$ and responds to the ciphertexts as

$$\begin{aligned} CT^* &= \left(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*\right) = \Big(M_b \\ &\oplus Ext\left(K^{t_1} e\left(y_1^{\gamma}, y_0\right)^{t_1}, s\right), y_0^{\sum_{i=1}^{k} T_i^*} g^{s_2 t_2}, y_0^t g^{s_2 t_3}, g^{s_2}, \\ &y_0^{t_1}, s\Big), \end{aligned} \tag{35}$$

where $b \in \{0,1\}$.

(v) Phase 2: $\mathscr{C}$ answers the queries in the same way as phase 1 with the added restriction that the $\mathscr{A}$ can not execute leakage queries.

(vi) Guess: $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$ and wins if $b' = b$.

From the above game, we can see that if $T = e(g,g)^{\alpha^{n+1}c}$, $\mathscr{C}$ is playing ***Game 1***. The challenge ciphertexts are valid encryption to M_b. In fact, let $c = s_1$. Then one can obtain

$$\begin{aligned} C_0^* &= M_b \oplus Ext\left(K^{t_1} e\left(y_1^{\gamma}, y_0\right)^{t_1}, s\right) \\ &= M_b \oplus Ext\left(e\left(g,g\right)^{\alpha^{n+1} c t_1} e\left(y_1^{\gamma}, y_0\right)^{t_1}, s\right) \\ &= M_b \oplus Ext\left(e\left(g^{\alpha^n}, g^{\alpha c}\right)^{t_1} e\left(y_1^{\gamma}, y_0\right)^{t_1}, s\right) \\ &= M_b \oplus Ext\left(e\left(y_n, y_1\right)^{t_1 c} e\left(g^{\gamma}, y_1\right)^{t_1 c}, s\right) \\ &= M_b \oplus Ext\left(e\left(y_n g^{\gamma}, y_1^{t_1}\right)^{c}, s\right) \\ &= M_b \oplus Ext\left(e\left(g_1, g_2\right)^{c}, s\right) \\ &= M_b \oplus Ext\left(e\left(g_1, g_2\right)^{s_1}, s\right), \\ C_1^* &= y_0^{\sum_{i=1}^{k} T_i^*} g^{s_2 t_2} = \left(\prod_{i=1}^{k} h_{in}\right)^{c} u^{s_2} = \left(\prod_{i=1}^{k} h_{in}\right)^{s_1} u^{s_2}, \\ C_2^* &= y_0^t g^{s_2 t_3} = w^c x^{s_2} = w^{s_1} x^{s_2}, \\ C_3^* &= g^{s_2}, \\ C_4^* &= y_0^{t_1} = v^c = v^{s_1}, \\ C_5^* &= s. \end{aligned} \tag{36}$$

Otherwise, K is a random element in G_T; $\mathscr{C}$ is playing ***Game 2***. Thus, ***Game 1*** and ***Game 2*** are computationally indistinguishable. □

Lemma 5. *Suppose the decisional linear assumption holds. Then **Game 2** and **Game 3** are indistinguishable.*

Proof. Suppose there is adversary $\mathscr{A}$ that can distinguish between ***Game 2*** and ***Game 3*** with advantage ε. Then a challenge $\mathscr{C}$ will be made to solve the decision linear problem.

$\mathscr{C}$ receives a challenge tuple

$$\begin{aligned} &\left(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n}, g^{z_2^{n+2}}, \ldots, g^{z_2^{2n}}, g^{z_3}, g^{z_4}, g^{z_4 z_2}, \ldots,\right. \\ &\left. g^{z_2^n z_4}, K\right), \end{aligned} \tag{37}$$

K is either $g^{z_1(z_3+z_4)}$ or a random element of G. $\mathscr{C}$ interacts with $\mathscr{A}$ as follows:

(i) Init: The adversary $\mathscr{A}$ gives the challenge identity $ID^* = (v_1^*, \ldots, v_k^*)$ to the challenger $\mathscr{C}$ where $k \le l$.

(ii) Setup: $\mathscr{C}$ randomly chooses $t, t_1, t_3, \gamma, \alpha_{ij}, \beta_{ij} \in Z_p^*$ where $1 \le i \le l$, $1 \le j \le n$. It sets

$$\begin{aligned} v &= g^{t_1}, \\ g_1 &= g^{t_1 z_2}, \\ u &= g^{z_4 \sum_k^{i=1} T_i^*}, \\ w &= g^{t}, \\ x &= g^{t_3}, \\ g_2 &= g^{z_2^n} g^{\gamma}, \end{aligned} \tag{38}$$

where $T_i^* = T(v_i^*)$. The public key parameters are $PK = \{g, g_1, g_2, v, u, w, x\}$. The master secret key is $MSK = g_2^{z_2} = y_1^{\gamma} g^{z_2^{n+1}}$ which is unknown to $\mathscr{C}$, where $y_i = g^{z_2^i}$.

(iii) Phase 1: $\mathscr{A}$ adaptively queries $\mathscr{C}$ with $ID = (v_1, \ldots, v_k)$ where $ID \neq ID^*$ and ID is not a prefix of ID^*. This condition ensures that there is $j \in \{1, \ldots, k\}$ such that $v_j \neq v_j^*$. $\mathscr{C}$ produces the private key corresponding to the identity $ID_j = (v_1, \ldots, v_j)$ where j denotes the first element such that $v_j \neq v_j^*$. Let τ be the number of sites such that $v_{ji} = v_{ji}^*$ in v_j. To respond to the query, $\mathscr{C}$ produces the auxiliary parameters as follows. For $1 \le i \le j$,

$$\begin{aligned} h_{i1} &= g^{\alpha_{i1}^{v_{i1}} \beta_{i1}^{1-v_{i1}}} \quad if\ v_{i1} \neq v_{i1}^*, \\ h_{i1} &= \left(g^{z_2}\right)^{\alpha_{i1}^{v_{i1}} \beta_{i1}^{1-v_{i1}}} \quad if\ v_{i1} = v_{i1}^*. \\ h_{i2} &= h_{i1}^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} \neq v_{i2}^*, \\ h_{i2} &= \left(g^{z_2}\right)^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} = v_{i2}^* \cap v_{i1} \neq v_{i1}^*, \\ h_{i2} &= \left(g^{z_2^2}\right)^{\alpha_{i2}^{v_{i2}} \beta_{i2}^{1-v_{i2}}} \quad if\ v_{i2} = v_{i2}^* \cap v_{i1} = v_{i1}^*. \end{aligned} \tag{39}$$

Finally, the auxiliary information parameters can be computed as follows.

$$\begin{aligned} h_{1n} &= y_n^{T(v_1)}, \\ &\ldots, \\ h_{(j-1)n} &= y_n^{T(v_{j-1})}, \\ h_{jn} &= y_{\tau}^{T(v_j)}, \end{aligned} \tag{40}$$

where

$$\begin{aligned} T(v_i) &= \prod_{j=1}^{n} \alpha_{ij}^{v_{ij}} \beta_{ij}^{1-v_{ij}}, \\ y_i &= g^{z_2^i}, \\ & 1 \le i \le j,\ \tau \le n. \end{aligned} \tag{41}$$

$\mathscr{C}$ randomly chooses $r_1' \in Z_p$ and sets $r_1 = r_1' - z_2^{n-\tau+1}/T(v_j)$. The private keys corresponding to the identity ID_j are simulated as follows.

$$\begin{aligned} d_{j0} &= y_1^{\gamma} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \left(y_{\tau}^{T(v_j)}\right)^{r_1'}, \\ d_{j1} &= g^{r_1'} y_{n-\tau+1}^{-1/T(v_j)}, \\ d_{j2} &= g^{r_1' t_1} y_{n-\tau+1}^{-t_1/T(v_j)}, \\ d_{j3} &= g^{r_1' t} y_{n-\tau+1}^{-t/T(v_j)}, \\ d_{j4} &= u^{r_1' t_1} y_{n-\tau+1}^{-t_1 z_4 \sum_{i=1}^{k} T_i^*/T(v_j)}, \\ d_{j5} &= x^{r_1' t_1} y_{n-\tau+1}^{-t_1 t_3/T(v_j)}. \end{aligned} \tag{42}$$

In fact,

$$\begin{aligned} d_{j0} &= y_1^{\gamma} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \left(y_{\tau}^{T(v_j)}\right)^{r_1'} \\ &= y_{n+1} y_1^{\gamma} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_{\tau}^{T(v_j)}\right)^{r_1'} y_{n+1}^{-1} \\ &= g_2^{z_2} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_{\tau}^{T(v_j)}\right)^{r_1'} y_{n+1}^{-1} \\ &= g_2^{\alpha} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_{\tau}^{T(v_j)}\right)^{r_1'} \left(y_{\tau}^{T(v_j)}\right)^{-z_2^{n-\tau+1}/T(v_j)} \\ &= g_2^{\alpha} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{r_1'} \left(\prod_{i=1}^{j-1} y_{2n-\tau+1}^{-T(v_i)/T(v_j)}\right) \\ &\quad \cdot \left(y_{\tau}^{T(v_j)}\right)^{(r_1' - z_2^{n-\tau+1}/T(v_j))} \\ &= g_2^{\alpha} \left(\prod_{i=1}^{j-1} y_n^{T(v_i)}\right)^{(r_1' - z_2^{n-\tau+1}/T(v_j))} \\ &\quad \times \left(y_{\tau}^{T(v_j)}\right)^{(r_1' - z_2^{n-\tau+1}/T(v_j))} \\ &= g_2^{\alpha} \left(\prod_{i=1}^{j} h_{in}\right)^{(r_1' - z_2^{n-\tau+1}/T(v_j))} = g_2^{\alpha} \left(\prod_{i=1}^{j} h_{in}\right)^{r_1}. \end{aligned} \tag{43}$$

In addition,

$$\begin{aligned} d_{j1} &= g^{r_1'} y_{n-\tau+1}^{-1/T(v_j)} = g^{r_1}, \\ d_{j2} &= g^{r_1' t_1} y_{n-\tau+1}^{-t_1/T(v_j)} = v^{r_1}, \\ d_{j3} &= g^{r_1' t} y_{n-\tau+1}^{-t/T(v_j)} = v^{r_1} = w^{r_1}, \\ d_{j4} &= u^{r_1' t_1} y_{n-\tau+1}^{-t_1 z_4 \sum_{i=1}^{k} T_i^*/T(v_j)} = u^{r_1 t_1}, \\ d_{j5} &= x^{r_1' t_1} y_{n-\tau+1}^{-t_1 t_3/T(v_j)} = x^{r_1 t_1}. \end{aligned} \tag{44}$$

Then we can obtain

$$\begin{aligned} d_{ID_j} &= \left(d_{j0}, d_{j1}, d_{j2}, d_{j3}, d_{j4}, d_{j5}\right) \\ &= \left(g_2^{\alpha} \left(\prod_{i=1}^{j} h_{in}\right)^{r_1}, g^{r_1}, v^{r_1}, w^{r_1}, u^{r_1 t_1}, x^{r_1 t_1}\right). \end{aligned} \tag{45}$$

$\mathscr{C}$ also produces D_{ID_j}. $\mathscr{C}$ uses d_{ID_j} to derive a private key for the descendant identity ID_k and gives $\mathscr{A}$ the result.

Then, $\mathscr{A}$ submits the leak queries to $\mathscr{C}$.

(iv) Challenge: $\mathscr{A}$ selects two messages M_0, M_1 on which it wishes to be challenged. $\mathscr{C}$ first produces the auxiliary parameters as $h_{in} = g^{z_1 T_i^*}$ for challenge identity ID^*, where $T_i^* = T(v_i^*)$. $\mathscr{C}$ then randomly chooses $R_0 \in G_T$ and a random seed $s \in \{0,1\}^t$ and responds to the ciphertexts as

$$\begin{aligned} CT^* &= \left(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*\right) \\ &= \left(R_0, K^{\sum_{i=1}^{n} T_i^*}, g^{z_3 t} g^{z_1 z_3}, g^{z_1}, g^{t_1 z_3}, s\right). \end{aligned} \tag{46}$$

(v) Phase 2: $\mathscr{C}$ answers the queries in the same way as phase 1 with the added restriction that $\mathscr{A}$ can not execute leakage queries.

(vi) Guess: $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$ and wins if $b' = b$.

From the above game, we can see that if $K = g^{z_1(z_3+z_4)}$, $\mathscr{C}$ is playing ***Game 2***. In fact, let $z_3 = s_1, z_1 = s_2$. Then one can obtain

$$\begin{aligned} C_1^* &= K^{\sum_{i=1}^{n} T_i^*} = \left(g^{z_1(z_3+z_4)}\right)^{\sum_{i=1}^{n} T_i^*} \\ &= \left(\left(g^{z_1}\right)^{\sum_{i=1}^{n} T_i^*}\right)^{z_3} \left(\left(g^{z_4}\right)^{\sum_{i=1}^{k} T_i^*}\right)^{z_1} \\ &= \left(\prod_{i=1}^{k} h_{in}\right)^{s_1} u^{s_2}, \\ C_2^* &= g^{z_3 t} g^{z_1 z_3} = w^{s_1} x^{s_2}, \\ C_3^* &= g^{z_1} = g^{s_2}, \\ C_4^* &= g^{t_1 z_3} = v^{s_1}, \\ C_5^* &= s. \end{aligned} \tag{47}$$

Otherwise, K is a random element in G, and $\mathscr{C}$ is playing ***Game 3***. Thus, ***Game 2*** and ***Game 3*** are computationally indistinguishable. □

Lemma 6. *Suppose the decisional linear assumption holds. Then **Game 3** and **Game 4** are indistinguishable.*

Proof. This proof is similar to Lemma 5. $\mathscr{C}$ receives a challenge tuple

$$\begin{aligned} &\left(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n}, g^{z_2^{n+2}}, \ldots, g^{z_2^{2n}}, g^{z_3}, g^{z_4}, g^{z_4 z_2}, \ldots,\right. \\ &\left. g^{z_2^n z_4}, g^{z_1 z_2}, \ldots, g^{z_2^n z_1}, K\right), \end{aligned} \tag{48}$$

K is either $g^{z_1(z_3+z_4)}$ or a random element of G. $\mathscr{C}$ interacts with $\mathscr{A}$ as follows:

(i) Init: adversary $\mathscr{A}$ gives the challenge identity $ID^* = (v_1^*, \ldots, v_k^*)$ to the challenger $\mathscr{C}$ where $k \le l$.

(ii) Setup: $\mathscr{C}$ randomly chooses $t, t_1, t_2, \gamma, \alpha_{ij}, \beta_{ij} \in Z_p^*$ where $1 \le i \le l$, $1 \le j \le n$. It sets

$$\begin{aligned} v &= g^{t_1}, \\ g_1 &= g^{t_1 z_2}, \\ u &= g^{t_2}, \\ w &= g^{t z_1}, \\ x &= g^{t z_4}, \\ g_2 &= g^{z_2^n} g^{\gamma}. \end{aligned} \tag{49}$$

The public key parameters are $PK = \{g, g_1, g_2, v, u, w, x\}$. The master secret key is $MSK = g_2^{z_2} = y_1^{\gamma} g^{z_2^{n+1}}$ which is unknown to $\mathscr{C}$, where $y_i = g^{z_2^i}$.

(iii) Phase 1: this section is similar to Lemma 5.

(iv) Challenge: $\mathscr{A}$ selects two messages M_0, M_1 on which it wishes to be challenged. $\mathscr{C}$ randomly chooses $R_0 \in G_T$, $R_1 \in G$, and a random seed $s \in \{0,1\}^t$ and responds to the ciphertexts as

$$\begin{aligned} CT^* &= \left(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*\right) \\ &= \left(R_0, R_1, K^t, g^{z_1}, g^{t_1 z_3}, s\right). \end{aligned} \tag{50}$$

(v) Phase 2: $\mathscr{C}$ answers the queries in the same way as phase 1 with the added restriction that $\mathscr{A}$ can not execute leakage queries.

(vi) Guess: $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$ and wins if $b' = b$.

From the above game, we can see that if $K = g^{z_1(z_3+z_4)}$, $\mathscr{C}$ is playing ***Game 3***. In fact, let $z_3 = s_1, z_1 = s_2$. Then one can obtain

$$\begin{aligned} C_2^* &= K^t = \left(g^{z_1(z_3+z_4)}\right)^t = g^{tz_1z_3}g^{tz_1z_4} = w^{s_1}x^{s_2}, \\ C_3^* &= g^{z_1} = g^{s_2}, \\ C_4^* &= g^{t_1z_3} = v^{s_1}, \\ C_5^* &= s. \end{aligned} \tag{51}$$

Otherwise, K is a random element in G, and $\mathscr{C}$ is playing ***Game 4***. Thus, ***Game 3*** and ***Game 4*** are computationally indistinguishable. □

Theorem 7. *If the decision $(n+1)$-BDHE assumption and the decisional linear assumption hold, then our anonymous HIBE scheme is $\ell(\lambda)$-leakage resilience secure.*

5.2. Leakage Resilience Analysis. Let V be used to represent a view that adversary $\mathscr{A}$ sees without leakage, we have $\widetilde{H}_\infty(\mathscr{A} \mid V) = \log p$. From the above leakage-resilient security model, one can know that, for the challenge identity ID^*, the adversary can get the most $\ell(\lambda)$ leak information when doing leak queries. We set $\ell(\lambda)$ as ξ bit; in other words, $\ell(\lambda)$ has 2^ξ values. From Lemma 2, one can obtain

$$\widetilde{H}_\infty(\mathscr{A} \mid (\ell(\lambda), V)) \geq \widetilde{H}_\infty(\mathscr{A} \mid V) - \xi = \log p - \xi. \tag{52}$$

Therefore, as long as the extractor's strength is $(\log p - \xi, \varepsilon)$, one can obtain

$$\begin{aligned} &SD\left(\left(Ext\left(e(g_1, g_2)^{s_1}, s\right), s, \ell(\lambda), V\right),\right. \\ &\left.(U, s, \ell(\lambda), V)\right) \leq \varepsilon, \end{aligned} \tag{53}$$

where U is uniform distribution and $s \in \{0,1\}^t$. The premise is that extractor performance is good enough; one can obtain $\xi \approx \log p$. Hence the distance between $C_0 = M_b \oplus Ext(e(g_1, g_2)^{s_1}, s)$ and uniform distribution is ε and the statistical distance between two ciphertexts is at most 2ε. Therefore, no PPT adversary can distinguish the two challenge ciphertexts with the advantage of more than 2ε. The leakage ratio of our scheme is

$$\rho = \frac{\ell(\lambda)}{(6\log p)} = \frac{\xi}{(6\log p)} \approx \frac{\log p}{(6\log p)} = \frac{1}{6}. \tag{54}$$

We compare our work with schemes [24, 35, 54] in Table 2, where *pk.size*, *sk.size*, *c.size*, and *LR* mean the public key size, the secret key size, the ciphertext size, and leakage-resilience, respectively. We define l as the maximum depth of HIBE, k represents the user identity depth, and the symbol "-" represents the fact that the corresponding scheme does not have this feature. It is noted that our scheme supports anonymity and leakage-resilience where both private keys and ciphertext have a constant size.

Our scheme has no obvious advantage in computational efficiency, but the public key length and private key length of our HIBE scheme are both in $O(1)$ time. However, we mainly solve the problem of key leakage in the acceptable range between computational efficiency and security balance.

Table 2: Comparisons of different schemes.

Scheme	*pk.size*	*sk.size*	*c.size*	Anonymity	LR
[35]	$O(l)$	$O(l)$	$O(1)$	√	-
[24]	$O(1)$	$O(1)$	$O(1)$	√	-
[55]	$O(1)$	$O(1)$	$O(1)$	-	√
Ours	$O(1)$	$O(1)$	$O(1)$	√	√

6. Conclusion and Future Work

In this paper, we present a secure s-health system based on a leakage-resilient anonymous HIBE scheme in the bounded-leakage model. Our scheme can protect the patient's privacy well, even when the private key is partially leaked. Our system also achieves the safe transmission of the patient's EHRs in the case of leakage attacks. And we provide an example to show the systems feasibility. The proposed scheme was proved to be secure against chosen plaintext attacks in the standard model under the Diffie-Hellman exponent assumption and decisional linear assumption. However, the doctors may reveal the privacy of patients in a malicious way; thus, in the future work, we can increase tracking technology to limit doctors' malicious information disclosure. In the future work, we can also study how to construct a secure s-health system which allows the master-key leakage.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by National Key R&D Program of China (no. 2017YFB0802000), National Natural Science Foundation of China (nos. 61772418, 61472472, and 61402366), and Natural Science Basic Research Plan in Shaanxi Province of China (nos. 2018JZ6001, 2015JQ6236, 2016JM6033, and 2015JQ6262). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications.

References

[1] J. Li, L. Wang, and Z. Huang, "Verifiable Chebyshev Maps-Based Chaotic Encryption Schemes with Outsourcing Computations in the Cloud/Fog Scenarios," *Concurrency and Computation: Practice and Experience*, 2018.

[2] L. Sun, Z. Li, Q. Yan, W. Srisa-An, and Y. Pan, "Sigpid: significant permission identification for android malware detection," in *Proceedings of the International Conference on Malicious and Unwanted Software*, pp. 1–8, 2017.

[3] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its

application in blockchain," *IEEE Access*, vol. PP, no. 99, pp. 1-1, 2018.

[4] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

[5] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowledge-Based Systems*, vol. 79, pp. 18–26, 2015.

[6] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[7] R. Xie, C. He, D. Xie, C. Gao, and X. Zhang, "A Secure Ciphertext Retrieval Scheme against Insider KGAs for Mobile Devices in Cloud," *Security and Communication Networks*, vol. 2018.

[8] Y. Zhang, J. Li, X. Chen, and H. Li, "Anonymous attribute-based proxy re-encryption for access control in cloud computing," *Security and Communication Networks*, vol. 9, no. 14, pp. 2397–2411, 2016.

[9] C. Yuan, X. Li, Q. J. Wu, J. Li, and X. Sun, "Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis," *Computers Materials & Continua*, vol. 53, no. 4, pp. 357–371, 2015.

[10] J. Li, X. Chen, S. S. M. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network Computer Applications*, 2018.

[11] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[12] P. Li, J. Li, Z. Huang et al., "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.

[13] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute-based encryption supporting efficient decryption test," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, pp. 511–516, ACM, 2013.

[14] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

[15] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computing*, no. 1, pp. 1–10, 2017.

[16] Y. Dodis and K. Pietrzak, *Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks*, Springer, Berlin, Heidelberg, Germany, 2010.

[17] J. A. Halderman, S. D. Schoen, N. Heninger et al., "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2008.

[18] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," *International Cryptology Conference on Advances in Cryptology*, pp. 104–113, 1996.

[19] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," *Ches May*, vol. 2162, pp. 251–261, 2001.

[20] D. Boneh, R. A. DeMillo, and R. J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, Springer, Berlin, Heidelberg, Germany, 1997.

[21] Y. H. Zhang, X. F. Chen, H. Li, and J. Cao, "Identity-based construction for secure and efficient handoff authentication schemes in wireless networks," *Security and Communication Networks*, vol. 5, no. 10, pp. 1121–1130, 2012.

[22] J. Li, X. Chen, X. Huang et al., "Secure distributed deduplication systems with improved reliability," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3569–3579, 2015.

[23] C. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," *Information Sciences*, 2018.

[24] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Compact Anonymous Hierarchical Identity-Based Encryption with Constant Size Private Keys," *Computer Journal*, vol. 59, no. 4, pp. 452–461, 2018.

[25] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[26] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Efficient attribute-based data sharing in mobile clouds," *Pervasive and Mobile Computing*, vol. 28, pp. 135–149, 2016.

[27] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.

[28] A. Shamir, *Identity-based cryptosystems and signature schemes*, vol. 21 of *Lecture Notes in Computer Science*, 2 edition, 1984.

[29] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on computers*, vol. 64, no. 2, pp. 425–437, 2015.

[30] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2002, International Conference on the Theory and Application of Cryptology and Information Security*, pp. 548–566, Queenstown, New Zealand, December, 2002.

[31] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques*, pp. 440–456, 2005.

[32] B. Waters, "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions," *International Cryptology Conference on Advances in Cryptology*, vol. 5677, pp. 619–636, 2009.

[33] J. H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, "Anonymous hierarchical identity-based encryption with constant size ciphertexts," in *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography*, vol. 5443, pp. 215–234, PKC, 2009.

[34] J. H. Seo and J. H. Cheon, "Fully secure anonymous hierarchical identity-based encryption with constant size ciphertexts," *Iacr Cryptology Eprint Archive*, vol. 2011, no. 2011, pp. 215–234, 2011.

[35] J. H. Park and D. H. Lee, "Anonymous hibe: Compact construction over prime-order groups," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2531–2541, 2013.

[36] S. C. Ramanna and P. Sarkar, *Anonymous Constant-Size Ciphertext HIBE from Asymmetric Pairings*, Springer, Berlin, Heidelberg, Germany, 2013.

[37] F. W. Dillema and S. Lupetti, "Rendezvous-based access control for medical records in the pre-hospital environment," in *Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments*, pp. 1–6, ACM, 2007.

[38] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Proceedings of the Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268–275, IEEE, 2010.

[39] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare," in *Proceedings of the Distributed Computing Systems (ICDCS), 2011 31st International Conference on*, pp. 373–382, 2011.

[40] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks," in *Proceedings of the IEEE International Conference on Distributed Computing Systems*, pp. 224–233, 2012.

[41] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 1927–1941, 2014.

[42] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for Naked healthcare environment," *IEEE International Conference on Communications*, 2017.

[43] A. Sudarsono, M. Yuliana, and H. A. Darwito, "A secure data sharing using identity-based encryption scheme for e-healthcare system," in *Proceedings of the International Conference on Science in Information Technology*, pp. 429–434, 2017.

[44] Y. Zhang, J. Li, D. Zheng, X. Chen, and H. Li, "Towards privacy protection and malicious behavior traceability in smart health," *Personal & Ubiquitous Computing*, vol. 21, no. 8, pp. 1–16, 2017.

[45] M. Dawoud and D. T. Altilar, "Cloud-based E-health systems: Security and privacy challenges and solutions," in *Proceedings of the International Conference on Computer Science and Engineering*, pp. 861–865, 2017.

[46] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2017.

[47] M. A. Sahi, H. Abbas, K. Saleem et al., "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2018.

[48] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," *IEEE Symposium on Foundations of Computer Science*, pp. 293–302, 2008.

[49] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, *Simultaneous hardcore bits and cryptography against memory attacks*, vol. 5444, Springer, Berlin, Heidelberg, Germany, 2009.

[50] M. Naor and G. Segev, "Public-key cryptosystems resilient to key leakage," *International Cryptology Conference on Advances in Cryptology*, vol. 5677, pp. 18–35, 2009.

[51] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs, "Public-key encryption in the bounded-retrieval model," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 113–134, 2010.

[52] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical leakage-resilient identity-based encryption from simple assumptions," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 152–161, 2010.

[53] S. Li, F. Zhang, Y. Sun, and L. Shen, "Efficient leakage-resilient public key encryption from ddh assumption," *Cluster Computing*, vol. 16, no. 4, pp. 797–806, 2013.

[54] P. Liu, C. Hu, S. Guo, and Y. Wang, "Anonymous identity-based encryption with bounded leakage resilience," in *Proceedings of the IEEE International Conference on Advanced Information NETWORKING and Applications Workshops*, pp. 287–292, 2015.

[55] J. Li, M. Teng, Y. Zhang, and Q. Yu, "A leakage-resilient cca-secure identity-based encryption scheme," *Computer Journal*, vol. 59, no. 7, pp. 1066–1075, 2016.

[56] J. Quisquater and D. Samyde, *ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards*, Springer, Berlin, Heidelberg, Germany, 2001.

[57] D. M. Freeman, *Converting pairing-based cryptosystems from composite-order groups to prime-order groups*, vol. 2009 of *Lecture Notes in Computer Science*, Springer, Berlin, 2010.

[58] M. Abdalla, D. Catalano, and D. Fiore, "Verifiable random functions from identity-based key encapsulation," *EUROCRYPT*, pp. 554–571, 2009.

[59] X. Boyen and B. Waters, *Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)*, Springer, Berlin, Heidelberg, Germany, 2006.

[60] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," *Journal of Cryptology*, no. 4, p. 172, 2004.