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 Guo1

1National Engineering Laboratory for Wireless Security, Xi’an University of Posts and Telecommunications, Xi’an 710121, China
2Westone Cryptologic Research Center, Beijing 100070, China
3State 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

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 cannot 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-resistant 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

\[ SD(X, Y) = \frac{1}{2} \sum_{w \in \Omega} |Pr[X = w] - Pr[Y = w]|. \] (1)
The min-entropy of a random variable $X$ is defined as

$$H_{\text{co}}(X) = -\log \left( \max_x \Pr [X = x] \right).$$

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

$$\widetilde{H}_{\text{co}}(X | Y) = -\log \left( \mathbb{E}_{y \sim Y} \left[ 2^{H_{\text{co}}(X | Y)} \right] \right).$$

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

$$SD \left( (\mathbb{E} (X, S), S, Y), (U_{\text{pre}}, S, Y) \right) \leq \varepsilon,$$

where $S$ is uniform over $(0,1)^l$, we call polynomial-time function $\mathbb{E}$ an average-case $(k, \varepsilon)$-strong extractor.

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

$$\widetilde{H}_{\text{co}}(X | (Y, Z)) \geq \widetilde{H}_{\text{co}}(X | Z) - r.$$ 

### 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 $\alpha, \beta \in \mathbb{Z}_p^*$. We define the computational $(n + 1)$--BDHE problem [56] to be

**input**: $(g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2}) \in G$,

**output**: $e \left( g, y_0 \right)^{\alpha^{n+1}} = e \left( g, g \right)^{\alpha^{n+1} \beta}$.

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

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

$$Pr \left( \mathcal{B}' \left( K'', e \left( g, y_0 \right)^{\alpha^{n+1}} \right) = 0 \right) - Pr \left( \mathcal{B}' \left( K'', e \right) = 0 \right) \geq \varepsilon.$$
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 to be treated by the doctor named Carol to treat the illness together. And the system assigns Alice to Carol through the cloud, but Carol’s private key may have been leaked partly by malicious attackers through various forms of leakage attacks.

During the entire process, Bob sends Alice’s EHRs to Carol through the cloud, but Carol’s private key may have been leaked partly if the general system is used, Alice’s EHRs may be leaked, but our system 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 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 (identity) and then uploads it to the s-health cloud (SHC). Then B decrypts medical information with its own private key. The adversary 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 (Game-real) between an adversary $A$ and a challenger $C$.

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

(ii) Setup: $C$ computes $(PK, MSK) \leftarrow Setup(\lambda)$. $C$ gives $PK$ to $A$ and keeps $MSK$ to itself. $A$ 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 $d_{ID}(ID, d_{ID}, L_{ID})$. Let $\ell(\lambda)$ be a leakage parameter.

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

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

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{The generation of the private keys.}
\end{figure}
4. Secure s-Health System

4.1. A Leakage-Resilient Anonymous HIBE Scheme.

A Leakage-Resilient Anonymous HIBE scheme is defined as follows:

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

(ii) **KenGen**($PK, ID_j, d_{ID_{j-1}}$) → $d_{ID_j}$: 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**($PK, ID_j, M$) → $CT$: 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**($PK, d_{ID_j}, CT$) → $M$: 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 ⊥ if the ciphertext is invalid.

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 $A$’s advantage is negligible in the above game. We define $A$’s advantage to be

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

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

$$PK = \{g, g_1, g_2, v, u, x, w\}.$$  \hspace{1cm} (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 $\{\alpha_1, \ldots, \alpha_{1n}, \beta_1, \ldots, \beta_{1n}\} \in Z_p$ and produces the auxiliary parameters

$$h_{ii} = (h_{i(i-1)})^{\alpha_i} \beta_i^{-\gamma_i},$$  \hspace{1cm} (16)

where $h_{10} = g, 1 \leq i \leq n$, and $h_{1i}$ is outputted as the public key. Root PKG outputs the private key for $ID_1$ as
\[ d_{ID_k} = (d_{k0}, d_{k1}, d_{k2}, d_{k3}, d_{k4}, d_{k5}) \]
\[ = (g_{k0}^{a_l}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, g_{k4}^{i_1}, g_{k5}^{x_i}) \]  
(17)

and

\[ D_{ID_k} = (D_{k0}, D_{k1}, D_{k2}, D_{k3}, D_{k4}, D_{k5}) \]
\[ = (h_{k0}^{r_i}, h_{k1}^{f_i}, h_{k2}^{i_i}, h_{k3}^{s_i}, h_{k4}^{i_1}, h_{k5}^{x_i}) \]  
(18)

where \( r_1, r_2 \in \mathbb{Z}_p \) and \( D_{ID_k} \) are used to rerandomize the private keys.

(b) **Delegate**: For the \( k\)-th level user \( ID_k = (v_{i1}, \ldots, v_{i_k}) \) where \( k \leq l \), \( v_i = (v_{i1}, \ldots, v_{in}) \) and \( v_{ij} \in [0, 1] \), by using the private key \( d_{ID_{k-1}} \) corresponding to the \((k-1)\)-th level user \( ID_{k-1} = (v_{j1}, \ldots, v_{j_{k-1}}) \):

\[ d_{ID_{k-1}} = (d_{k-10}, d_{k-11}, d_{k-12}, d_{k-13}, d_{k-14}, d_{k-15}) \]
\[ = \left( g_{k0}^{r_i}, \prod_{i=1}^{k-1} h_{in}^{r_i}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, u_{k4}^{i_1}, x_{k5}^{x_i} \right) \]  
(19)

\[ D_{ID_{k-1}} = (D_{k-10}, D_{k-11}, D_{k-12}, D_{k-13}, D_{k-14}, D_{k-15}) \]
\[ = \left( h_{k0}^{r_i}, h_{k1}^{f_i}, h_{k2}^{i_i}, h_{k3}^{s_i}, h_{k4}^{i_1}, h_{k5}^{x_i} \right) \].  
(20)

PKG\(_k\) randomly chooses

\[ \{a_{k1}, \ldots, a_{kn}, \beta_{k1}, \ldots, \beta_{kn}\} \in \mathbb{Z}_p \]  
(21)

and it produces the auxiliary parameters

\[ h_{k0}^i = (h_{k(j-1)}^{a_{kj}})^{\beta_{kj}} \]
\[ = (g_{k0}^{r_i}, \prod_{i=1}^{k-1} h_{in}^{r_i}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, g_{k4}^{i_1}, g_{k5}^{x_i}) \]  
(22)

where \( h_{k0} = d_{(k-1)0}, h_{kn0} = D_{(k-1)0} \) and \( 1 \leq j \leq n. \)

Let \( h_{kn} = g_{k0}^{\prod_{i=1}^{k-1} h_{in}^{r_i}} \); then one can obtain

\[ h_{kn}^i = (h_{kn})^{f_i} \]  
and

\[ h_{kn}^i = (h_{kn})^{g_i} \].

PKG\(_k\) outputs the private key for \( ID_k \) as

\[ d_{ID_k} = (d_{k0}, d_{k1}, d_{k2}, d_{k3}, d_{k4}, d_{k5}) = \left( d_{(k-1)0}^{h_{kn0}} \right) \]

\[ \cdot (D_{(k-1)}h_{kn}^i)^{f_i}, d_{(k-1)}D_{(k-1)3}, d_{(k-1)4}D_{(k-1)5}) \]  
(23)

and

\[ D_{ID_k} = (D_{k0}, D_{k1}, D_{k2}, D_{k3}, D_{k4}, D_{k5}) \]
\[ = \left( D_{(k-1)}h_{kn}^i, D_{(k-1)1}, D_{(k-1)2}, D_{(k-1)3}, D_{(k-1)4}, D_{(k-1)5} \right) \]
\[ = \left( g_{k0}^{a_i}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, g_{k4}^{i_1}, g_{k5}^{x_i} \right) \]

\[ (\prod_{i=1}^{k} h_{in}^{r_i}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, g_{k4}^{i_1}, g_{k5}^{x_i}) \]

\[ = \left( g_{k0}^{a_i}, g_{k1}^{f_i}, g_{k2}^{i_i}, g_{k3}^{s_i}, g_{k4}^{i_1}, g_{k5}^{x_i} \right) \].

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

Encrypt: The encryptor randomly chooses \( s_1, s_2 \in \mathbb{Z}_p \) and a random seed \( s \in [0, 1]^t \). The encryptor creates the ciphertext as follows:

\[ CT = (C_0, C_1, C_2, C_3, C_4, C_5) = \left( M, \oplus Ext(e(g_1, g_2)^{s_1}, s), (\prod_{i=1}^{k} h_{in}^{r_i})^{s_1} \right) \]

\[ \cdot u^{s_2}, w^{s_2}, x^{s_2}, y^{s_1}, v^{s_1}, s \)  
(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

\[ M = Ext\left( e(d_{k0}, C_4) e(d_{k4}d_{k5}, C_3) e(d_{k3}, C_4) \right) \]

\[ e(C_1, d_{k2}) e(C_2, d_{k2}) \]  
(26)

\[ \oplus C_0. \]

4.3. **Correctness**. The correctness can be checked:

\[ e(d_{k0}, C_4) e(d_{k4}d_{k5}, C_3) e(d_{k3}, C_4) \]
\[ e(C_1, d_{k2}) e(C_2, d_{k2}) \]
\[ = e(g_2^{a_i}, \prod_{i=1}^{k} h_{in}^{r_i})^{s_1}, (ux)^{r_1}, g^{r_1} e(w^{r_1}, v^{r_1}) \]
\[ = e(g_1, g_2)^{s_1}. \]

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 Game\(_{real}\). 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 \( R_0 \in G_r \) 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-Boyan selective-ID scheme [60] and Abdalla’s security analysis [58]. Suppose there is adversary \( A \) that can distinguish between Game 1 and Game 2 with advantage \( \epsilon \). Then challenge \( \mathcal{C} \) will be made to solve the decision \((n + 1)\)-BDHE assumption.

\( \mathcal{C} \) receives a challenge tuple \((g, y_0, y_1, \cdots, y_m, y_{n+2}, \cdots, y_{2n+2}, k)\) where \( y_0 = g^{e_1}, y_i = g^{e_i} \) and \( k \) is either \( e(g, g)^{\alpha_{12}^*} \) or a random element of \( G_r \). \( \mathcal{C} \) interacts with \( A \) as follows:

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

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

\[
\begin{align*}
&v = g^{t_1}, \\
g_1 = y_1^{t_1}, \\
u = g^{t_1}, \\
x = g^{t_1}, \\
w = g^{t_1}, \\
g_2 = y_ng^{t_1}.
\end{align*}
\]

(28)

The public key parameters are \( PK = \{g, g_1, g_2, v, u, x, w\} \). The master secret key is \( MSK = g_2^a = y_1^y \), which is unknown to \( \mathcal{C} \).

(iii) **Phase 1:** \( A \) adaptively queries \( \mathcal{C} \) 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 \( v_j \neq v_j^* \). \( \mathcal{C} \) produces the private key corresponding to the identity \( ID_j = (v_1, \ldots, v_j) \), where \( j \) denotes the first element such that \( v_j \neq v_j^* \). Let \( r \) be the number of sites such that \( v_{j_i} = v_{j_i}^* \) in \( v_j \). To respond to the query, \( \mathcal{C} \) produces the auxiliary parameters as follows. For \( 1 \leq i \leq j \), compute

\[
\begin{align*}
h_{i1} = y_1^{\alpha_{i1}^*} & \quad \text{if } v_{i1} \neq v_{i1}^*, \\
h_{i2} = y_1^{\alpha_{i2}^*} & \quad \text{if } v_{i2} \neq v_{i2}^*, \\
h_{i3} = y_1^{\alpha_{i3}^*} & \quad \text{if } v_{i3} \neq v_{i3}^*, \\
h_{i4} = y_1^{\alpha_{i4}^*} & \quad \text{if } v_{i4} \neq v_{i4}^*, \\
h_{i5} = y_1^{\alpha_{i5}^*} & \quad \text{if } v_{i5} \neq v_{i5}^*, \\
h_{i6} = y_1^{\alpha_{i6}^*} & \quad \text{if } v_{i6} \neq v_{i6}^*. 
\end{align*}
\]

Finally, the auxiliary parameters can be computed as follows.

\[
\begin{align*}
h_{in} = y_n^T(v_i), \\
\vdots \\
h_{(i-1)n} = y_n^T(v_{i-1}), \\
h_{jn} = y_n^T(v_j),
\end{align*}
\]

(30)

where \( T(v_i) = \prod_{j=1}^{n+1} \alpha_{ij}^{-\alpha_{ij}^*} \), \( \text{for } 1 \leq i \leq j, \tau \leq n \). \( \mathcal{C} \) randomly chooses \( r_1 \in Z_p \) and sets \( r_1 = r_1 - \alpha_{n+1}^{n+1} \).

In fact,

\[
\begin{align*}
d_{j0} &= y_1^y \left( \prod_{i=1}^{j-1} y_i^T(v_i) \right) \left( \prod_{i=1}^{j-1} y_{2(n-r+1)}^T(v_i) \right) \left( y_T^T(v_j) \right)^{r_1}, \\
d_{j1} &= g^t y_{n-r+1}, \\
d_{j2} &= g^{r_1} y_{n-r+1}, \\
d_{j3} &= g^{r_1} y_{n-r+1}, \\
d_{j4} &= g^{r_1} y_{n-r+1}, \\
d_{j5} &= g^{r_1} y_{n-r+1}.
\end{align*}
\]


\[ g_2^a \left( \prod_{i=1}^{j-1} y_n^{T(v_i)} \right)^{r_i} \left( \prod_{i=1}^{j-1} y^{T(v_i)/T(v_j)} \right) \]

\[ \cdot \left( y^{T(v_j)} \right)^{r_i \cdot \alpha - r_j} \]

\[ = g_2^a \left( \prod_{i=1}^{j} y_n^{T(v_i)} \right)^{ \left( r_i - \alpha \cdot r_j + T(v_j) \right) } \]

\[ \times \left( y^{T(v_j)} \right)^{r_i \cdot \alpha - r_j} \]

\[ = g_2^a \left( \prod_{i=1}^{j} h_m \right)^{r_i} = g_2^a \left( \prod_{i=1}^{j} h_m \right)^{r_i} . \] (32)

In addition,

\[ d_{j1} = g^{r_1} y_n^{r_j - r - 1} = g^{r_1}, \]

\[ d_{j2} = g^{r_3} y_n^{r_j + r - 1} = v^{r_3}, \]

\[ d_{j3} = g^{r_1} y_n^{r_j + r - 1} = v^{r_1}, \]

\[ d_{j4} = g^{r_3} y_n^{r_j + r - 1} = u^{r_3}, \]

\[ d_{j5} = g^{r_1} y_n^{r_j + r - 1} = x^{r_1}. \] (33)

Then we can obtain

\[ d_{ID} = \left( d_{b0}, d_{j1}, d_{j2}, d_{j3}, d_{j4}, d_{j5} \right) \]

\[ = \left( g_2^a \left( \prod_{i=1}^{j} h_m \right)^{r_i}, g^{r_1}, v^{r_3}, u^{r_3}, x^{r_1}, x^{r_1} \right). \] (34)

\( \mathcal{C} \) also produces \( D_{ID} \). \( \mathcal{C} \) uses \( D_{ID} \) to derive a private key for the descendant identity \( ID_{x} \) and gives \( \mathcal{A} \) the result.

Then, \( \mathcal{A} \) submits the leak queries to \( \mathcal{C} \).

(iv) Challenge: \( \mathcal{A} \) selects two messages \( M_0, M_1 \) on which it wishes to be challenged. \( \mathcal{C} \) first produces the auxiliary parameters as \( h_n = g^{T(v_j)} \) for challenge identity \( ID^* \), where \( T(v_j) = T(v_j) \). \( \mathcal{C} \) then randomly chooses \( s_1, s_2 \in \mathbb{Z}_p \) and a random seed \( s \in \{0, 1\}^l \) and responds to the ciphertexts as

\[ CT^* = (C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*) = \left( M_b \oplus \text{Ext} \left( K^c e \left( y^{T(v_j)} y_0^{s_1} \right), s \right), y_0^{T(v_j)}, g^{s_1}, g^{s_2}, y_0^{T(v_j)}, s \right), \] (35)

where \( b \in \{0, 1\} \).

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

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

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

\[ C_0^* = M_b \oplus \text{Ext} \left( K^c e \left( y^{T(v_j)} y_0^{s_1} \right), s \right) = M_b \oplus \text{Ext} \left( e(g, g)^{a_i + 1} e \left( y^{T(v_j)} y_0^{s_1} \right), s \right) \]

\[ = M_b \oplus \text{Ext} \left( e(g^{a_i}, g^{a_i})^{s_1} e \left( y^{T(v_j)} y_0^{s_1} \right), s \right) \]

\[ = M_b \oplus \text{Ext} \left( e(y_n, y_0), s \right) \]

\[ = M_b \oplus \text{Ext} \left( e(g, g), s \right) \]

\[ = M_b \oplus \text{Ext} \left( e(g_1, g_2) \right), \] (36)

\[ C_1^* = y_0^{s_1} g^{s_2} = \left( \prod_{i=1}^{k} h_n \right)^{c} u^{s_1} = \left( \prod_{i=1}^{k} h_n \right)^{s_1} u^{s_1}, \]

\[ C_2^* = y_0^{s_2} g^{s_3} = u^{s_1} g^{s_3} = w^{s_1} x^{s_3}, \]

\[ C_3^* = g^{s_2}, \]

\[ C_4^* = y_0^{s_1} = v^{s_1}, \]

\[ C_5^* = s. \]

Otherwise, \( K \) is a random element in \( G_2 \); \( \mathcal{C} \) is playing Game 2. Thus, Game 1 and Game 2 are computationally indistinguishable. \( \square \)

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

Proof. Suppose there is adversary \( \mathcal{A} \) that can distinguish between Game 2 and Game 3 with advantage \( \epsilon \). Then a challenge \( \mathcal{C} \) will be made to solve the decision linear problem. \( \mathcal{C} \) receives a challenge tuple

\[ \left( g, g^{s_1}, g^{s_2}, g^{s_3}, \ldots, g^{s_{n-1}}, g^{s_0}, g^{s_1}, g^{s_2}, g^{s_3}, \ldots, \right), \]

\[ g^{s_{n+1}}, K \right). \] (37)

\( K \) is either \( g^{s_{n+1}} + r_{x+z_0} \) or a random element of \( G \). \( \mathcal{C} \) interacts with \( \mathcal{A} \) as follows:

(i) Init: The adversary \( \mathcal{A} \) gives the challenge identity \( ID^* = (v_1^*, \ldots, v_n^*) \) to the challenger \( \mathcal{C} \) where \( k \leq l \).
(ii) Setup: $\mathcal{C}$ randomly chooses $t, t_1, t_2, y, \alpha_{ij}, \beta_{ij} \in \mathbb{Z}_p^*$ where $1 \leq i \leq l, 1 \leq j \leq n$. It sets

$$v = g^t,$$

$$g_1 = g^{t_2z_1},$$

$$u = g^{t_1x_i},$$

$$w = g_j,$$

$$x = g^{t_3},$$

$$g_2 = g^{t_4y},$$

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 $MSK = g_2^z = y^*_1g^{\alpha_{i1}z_1}$ which is unknown to $\mathcal{C}$, where $y_1 = g^{t_1}$.

(iii) Phase 1: $\mathcal{C}$ adaptively queries $\mathcal{C}$ 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 $v_j \neq v_j^*$. $\mathcal{C}$ produces the private key corresponding to the identity $ID_j = (v_1, \ldots, v_j)$ where $j$ denotes the first element such that $v_j \neq v_j^*$. Let $\tau$ be the number of sites such that $v_{ij} = v_{ij}^*$ in $v_j$. To respond to the query, $\mathcal{C}$ produces the auxiliary parameters as follows. For $1 \leq i \leq j$,

$$h_1 = g^{z_1\alpha_{i1}^2\beta_{i1}^{\alpha_{i1}}} \text{ if } v_{i1} \neq v_{i1}^*,$$

$$h_1 = (g^{z_1\alpha_{i1}^2\beta_{i1}^{\alpha_{i1}}} V  \text{ if } v_{i1} = v_{i1}^*,$$

$$h_2 = h_1^2 \text{ if } v_{i2} \neq v_{i2},$$

$$h_2 = (g^{z_1\alpha_{i1}^2\beta_{i1}^{\alpha_{i1}}} V  \text{ if } v_{i2} = v_{i2}^* \cap v_{i1} \neq v_{i1}^*,$$

$$h_2 = (g^{z_1\alpha_{i1}^2\beta_{i1}^{\alpha_{i1}}} V  \text{ if } v_{i2} = v_{i2}^* \cap v_{i1} = v_{i1}^*,$$

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

$$h_{1n} = y_n^{T(v_n)},$$

$$\cdots,$$

$$h_{(j-1)n} = y_n^{T(v_{(j-1)n})},$$

$$h_{jn} = y_n^{T(v_j)};$$

where

$$T(v_j) = \prod_{i=1}^{n} a_i v_i^{1-v_i};$$

$$y_i = g^{z_1},$$

$1 \leq i \leq j, \tau \leq n.$

$\mathcal{C}$ randomly chooses $r_1' \in \mathbb{Z}_p$ and sets $r_1 = r_1' - z_2^{2\tau+1}/T(v_j)$. The private keys corresponding to the identity $ID_j$ are simulated as follows.

$$d_{j0} = y_{n+1}^j \prod_{i=1}^{j-1} y_{n+1}^{T(v_{i1})} \prod_{i=1}^{j-1} y_{2\tau+1}^{T(v_{i2})} y_{\tau}^{T(v_j)} r_1',$$

$$d_{j1} = g^{r_1' - T(v_j)} y_{n-1}^j,$$

$$d_{j2} = g^{r_1' - T(v_j)} y_{n-1}^j,$$

$$d_{j3} = g^{r_1'} y_{n-1}^j,$$

$$d_{j4} = u^{r_1'} - y_{n-1}^j y_{n-1}^j,$$

$$d_{j5} = x^{r_1'} y_{n-1}^j.$$
In addition,
\[ d_R = g^{i_1j_1 \cdot T_y} = g^1, \]
\[ d_R = g^{i_1j_1 \cdot T_y} = v^1, \]
\[ d_R = g^{i_1j_1 \cdot T_y} = v^1 = w^1, \] (44)
\[ d_R = u^{i_1j_1 \cdot T_y} = u^{i_1}, \]
\[ d_R = x^{i_1j_1 \cdot T_y} = x^{i_1}. \]

Then we can obtain
\[ d_{ID_j} = (d_{r0}, d_{r1}, d_{r2}, d_{r3}, d_{r4}, d_{r5}) = g_2^\phi \left( \prod_{i=1}^{j} h_{in} \right)^{r_j}, g^{i_1}, v^{i_1}, w^{i_1}, u^{i_1}, x^{i_1}. \] (45)

\( \mathcal{C} \) also produces \( D_{ID_j} \), \( \mathcal{C} \) uses \( D_{ID_j} \) to derive a private key for the descendant identity \( ID_k \) and gives \( \mathcal{A} \) the result.

Then, \( \mathcal{A} \) submits the leak queries to \( \mathcal{C} \).

(iv) Challenge: \( \mathcal{A} \) selects two messages \( M_0, M_1 \) on which it wishes to be challenged. \( \mathcal{C} \) first produces the auxiliary parameters as \( h_{in} = g^{i_1j_1} \) for challenge identity \( ID^* \), where \( T_y = T(v^1) \). \( \mathcal{C} \) then randomly chooses \( R_0 \) and a random seed \( s \in \{0, 1\}^l \) and responds to the ciphertexts as
\[ CT^* = (C_{00}, C_{10}, C_{20}, C_{30}, C_{40}, C_{50}) = (R_0, K^{\sum_i T_i}, g^{i_1}, g^{z_i}, g^{v^1}, g^{w^1}, s). \] (46)

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

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

From the above game, we can see that if \( K = g^{z_i \cdot (z_i + z_i)} \), \( \mathcal{C} \) is playing Game 2. In fact, let \( z_3 = s_1, z_1 = s_2 \). Then one can obtain
\[ C_1 = K^{\sum_i T_i} = (g^{z_i(z_1 + z_2)})^{\sum_i T_i} = (g^{z_1})^{\sum_i T_i}, \]
\[ C_2 = g^{z_i} \cdot z_i = w^1 \cdot x^s, \]
\[ C_3 = g^{z_1} = g^{s_2}, \]
\[ C_4 = g^{v_1} = v^1, \]
\[ C_5 = s. \] (47)

Otherwise, \( K \) is a random element in \( G \), and \( \mathcal{C} \) 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. \( \mathcal{C} \) receives a challenge tuple
\[ (g, g_1, g_2, ..., g_n, g_{n+1}, g_{n+2}, ..., g_{n+3}, g_{n+4}, g_{n+5}, g_{n+6}, ..., g_{n+7}, g_{n+8}, ...), \]
\[ g_{n+9}, g_{n+10}, ..., g_{n+12}, K), \] (48)

\( K \) is either \( g^{z_i(z_i + z_i)} \) or a random element of \( G \). \( \mathcal{C} \) interacts with \( \mathcal{A} \) as follows:

(i) Init: adversary \( \mathcal{A} \) gives the challenge identity \( ID^* = (v^1, ..., v^l) \) to the challenger \( \mathcal{C} \) where \( k \leq l \).

(ii) Setup: \( \mathcal{C} \) randomly chooses \( t, t_1, t_2, v, a_i, \beta_i \in Z\) where \( 1 \leq i \leq l, 1 \leq j \leq n \). It sets
\[ v = g^1, \]
\[ g_1 = g^{z_1}, \]
\[ u = g^{z_2}, \]
\[ w = g^{z_3}, \]
\[ x = g^{z_4}, \]
\[ g_2 = g^{z_5} g^y. \] (49)

The public key parameters are \( PK = \{g, g_1, g_2, v, u, w, x\} \). The master secret key is \( MSK = g_2^{z_1} = y g^{z_1} \) which is unknown to \( \mathcal{C} \), where \( y_i = g^{z_i} \).

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

(iv) Challenge: \( \mathcal{A} \) selects two messages \( M_0, M_1 \) on which it wishes to be challenged. \( \mathcal{C} \) randomly chooses \( R_0 \) and a random seed \( s \in \{0, 1\}^l \) and responds to the ciphertexts as
\[ CT^* = (C_{00}, C_{10}, C_{20}, C_{30}, C_{40}, C_{50}) = (R_0, R_1, K^{t}, g^{z_1}, g^{z_2}, s). \] (50)

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

(vi) Guess: \( \mathcal{A} \) outputs a bit \( b' \in \{0, 1\} \) and wins if \( b' = b \).
From the above game, we can see that if \( K = g^{z_1 z_2} z_3 \), \( \mathcal{E} \) is playing \textit{Game 3}. In fact, let \( z_3 = s_1, z_1 = s_2 \). Then one can obtain
\[
C_2^* = K' = (g^{z_1 z_2} z_3)^t = g^{z_2 z_3} = g^{z_3} z_2 = w_1 x^{s_1},
\]
\[
C_3^* = g^{z_3} = v^1, \tag{51}
\]
\[
C_4^* = s.
\]

Otherwise, \( K \) is a random element in \( G \), and \( \mathcal{E} \) is playing \textit{Game 4}. Thus, \textit{Game 3} and \textit{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 \( \mathcal{A} \) sees without leakage, we have \( H_\co(\mathcal{A} \mid V) = \log p \). 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 \( \xi \) bit; in other words, \( \ell(\lambda) \) has \( 2^\xi \) values. From Lemma 2, one can obtain
\[
H_\co(\mathcal{A} \mid (\ell(\lambda), V)) \geq H_\co(\mathcal{A} \mid V) - \xi = \log p - \xi. \tag{52}
\]
Therefore, as long as the extractor's strength is \( (\log p - \xi, \epsilon) \), one can obtain
\[
SD((\text{Ext}(e(g_1, g_2)^{y_1}, s), s, \ell(\lambda), V); (U, s, \ell(\lambda), V)) \leq \epsilon, \tag{53}
\]
where \( U \) is uniform distribution and \( s \in \{0, 1\}^t \). The premise is that extractor performance is good enough; one can obtain \( \xi = \log p \). Hence the distance between \( C_0 = M_u \oplus \text{Ext}(e(g_1, g_2)^{y_1}, s) \) and uniform distribution is \( \epsilon \) and the statistical distance between two ciphertexts is at most \( 2\epsilon \). Therefore, no PPT adversary can distinguish the two challenge ciphertexts with the advantage of more than \( 2\epsilon \). The leakage ratio of our scheme is
\[
\rho = \frac{\xi}{(6 \log p)} = \frac{\xi}{(6 \log p)} \approx \frac{1}{6}. \tag{54}
\]

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.

### 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, 2016J6033, and 2015JQ6262). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications.

### References


---

### Table 2: Comparisons of different schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>( pk.size )</th>
<th>( sk.size )</th>
<th>( c.size )</th>
<th>Anonymity</th>
<th>LR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[35]</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>[24]</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>[55]</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Ours</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>( O(1) )</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>


Security and Communication Networks


Submit your manuscripts at www.hindawi.com