Hindawi
Security and Communication Networks
Volume 2018, Article ID 6395362, 8 pages
https://doi.org/10.1155/2018/6395362

Research Article

A Source Hiding Identity-Based Proxy Reencryption Scheme for Wireless Sensor Network

Chunpeng Ge,[1] **Jinyue Xia**,[2] **Aaron Wu**,[3] **Hongwei Li**,[4] **and Yao Wang**[4]

[1]*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[2]*IBM, 3039 E Cornwallis Rd., Research Triangle Park, NC 27709, USA*
[3]*College of Computer Sciences, University of Illinois at Urbana Champaign, 1205 W. Nevada St. MC-137, Urbana, USA*
[4]*College of Computer Engineering, Jiangsu University of Technology, Changzhou, Jiangsu 213000, China*

Correspondence should be addressed to Chunpeng Ge; gecp@jsut.edu.cn

Received 31 May 2018; Accepted 2 October 2018; Published 17 October 2018

Guest Editor: Zhaoqing Pan

Wireless sensor network (WSN), which extends the typical Internet environment to Internet of Things, has been deployed in various environments such as safety monitoring, intelligent transportation, and smart home. In a WSN, encryption is typically used to protect data that are stored in wireless devices. However some features like data sharing can be affected if the traditional encryption is used. A secure mechanism should support a gateway of the network to directly convert a user's encrypted data (encrypted pollution data) to a new user's encryption without exposing the underlying plaintext data during the whole sharing phase. In this work, a new source hiding identity-based proxy reencryption scheme (SHIB-PRE) is proposed to deal with the issue. The proposed SHIB-PRE scheme supports a proxy (gateway or cloud server) to transform a user's encrypted date to a new user's ciphertext as long as the proxy has the proxy reencryption key. In SHIB-PRE, the encrypted pollution data is kept secure from the proxy and the relationship between a source ciphertext and a reencrypted ciphertext is concealed from the outside eavesdropper. In this paper, we give an introduction to the definition of a source hiding identity-based proxy reencryption and its chosen plaintext security model. Further, a concrete construction will be presented and proven chosen plaintext secure under the $q - DDHE$ assumption in the standard model.

1. Introduction

With the growth of wireless sensor devices, people are facing a formidable problem of huge sensor data management and maintenance [1, 2]. One cost-effective and convenient approach to resolve this issue is to deploy the sensor data on the cloud, for example, IBM cloud [3] and Amazon AWS [4]. People can adopt data encryption as an intuitive defense to ensure data confidentiality on the cloud [5]. By encrypting the sensor data and saving on the cloud, however, sharing sensor data within the wireless sensor network is limited. As a result, traditional public key encryption only guarantees the confidentiality of wireless sensor data, yet it is frustrating with the data sharing functionality.

Considering the following scenario, we will need a secure mechanism that supports a gateway of the network to directly convert a user's encrypted data (encrypted pollution data) to a new user's encrypted data without revealing the underlying plaintext data. Suppose many wireless sensor nodes are deployed in a wireless pollution sensor network to monitor the campus air quality. All sensor nodes send their monitoring data to the sink node and then send to the cloud through the gateway. For the purpose of confidentiality, we could encrypt the monitoring data before sending it to the sink node. In some situations, the campus administrator Alice may want to cooperate with the government institute researcher Bob to analyze the environment. As the data is encrypted by Alice's public key, Bob cannot decrypt the encryption to get the underlying plaintext due to the fact that he does not access to Alice's private key. What we can do in this case is that let the campus administrator Alice fetch the secret data off the cloud and then reencrypt the data with Bob's public key. However, it can significantly increase Alice workload and violates the original intention of cloud

computing, leaving heavy workload to the cloud. What is worse is that Alice should be online all time during each sharing phase. Another native solution is that Alice can store the private key in cloud. Thus the cloud can perform the download-decrypt-reencrypt work instead of Alice. But, it may be a disaster if the cloud is disclosed as the attacker can use Alice's private key.

In addition to secure data sharing, another security requirement for above scenario is privacy preservation. If the government system is disclosed, the campus' identity should not be revealed. This privacy-preserving property enables that, even if the government system is assailed by an adversary, the adversary can not know who is sharing the data with the government system. This requires the relationship between the campus and the government system can not be revealed by an attacker.

Therefore, a new public key encryption mechanism is desired to support data sharing and privacy preservation at the same time. Enabling the confidentiality of data and preserving the privacy without losing efficiency [6] are an important problem to be issued. In this work, we focus on solving these elusive problems by presenting a novel notion of source hiding identity-based proxy reencryption. In our proposed source hiding identity-based proxy reencryption scheme, a proxy (gateway or cloud server) with a proxy reencryption key can convert a delegator's (campus) ciphertext to a delegate's (government institute researcher) ciphertext without exposing the plaintext. At the meanwhile, an outsider eavesdropper can not gain the relationship between the original ciphertext and the reencrypted ciphertext.

In related work, proxy reencryption (PRE) was proposed to enable a semitrusted proxy to convert Alice's ciphertext to Bob's ciphertext by a reencryption key [7]. Proxy reencryption has been applied into several places, such as secure email forwarding [7, 8] and cloud computing [9]. Green et al. [10] introduced identity-based proxy reencryption in which a user's public key is viewed as his identity. After their work, a great number of identity-based proxy reencryptions have came out [11–13] to deal with the efficiency and security property. An AB-PRE scheme was presented to apply attribute-based setting to proxy reencryption [14]. Luo, Hu, and Chen [15] revealed another scheme to provide "AND" gates on both positive and negative attributes. Later on, a ciphertext-policy attribute-based proxy reencryption (CPAB-PRE) [16, 17] was presented to support a monotonic access formula in the selective model. Further, they enhanced its security in the adaptive model [18]. Meanwhile, Ge et al. [19, 20] presented two key-policy attribute-based proxy reencryption (KPAB-PRE) schemes in both the selective and adaptive model, respectively. Recently, a DFA-based proxy reencryption scheme [21] allows the access to be described as a DFA. Unfortunately, none of these schemes support the functionality of privacy-preserving keyword search.

To capture the source hiding property, Emura, Miyaji, and Omote [22] introduced the notion of source hiding and they presented the first source hiding IB-PRE scheme in the random oracle model. However, their proof is only a heuristic argument and might lead to the scheme insecure [23]. Furthermore, the previous source hiding scheme [22] is found not collusion resistant. As a result, if a proxy colludes a set of delegates, the delegator's message is revealed as well as the delegator's private key.

1.1. Our Contribution. To address above problems [22], this work presents a CPA secure collusion resistant source hiding identity-based proxy scheme. Additionally, we prove the security without random oracles. More specifically, a proxy and a set of delegates can only collude to reveal the plaintext but not the delegator's private key. The paper organizes as follows: first we describe our scheme, second we prove our scheme secure in the standard model, and finally we show it is collusion resistant.

2. Preliminaries

2.1. Bilinear Map. G and G_T denote two multiplicative cyclic groups with the same prime order p. g is a generator of group G. A bilinear pairing is a bilinear map $e : G \times G \longrightarrow G_T$ with the following properties [24]:

(1) $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $a, b \overset{R}{\leftarrow} Z_p^*$ and $g_1, g_2 \in G$.

(2) $e(g, g) \neq 1$.

(3) There is an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1, g_2 \in G$.

2.2. Complexity Assumption. Our proposed system security relies on the truncated q decisional Diffie-Hellman exponent (q-DDHE) assumption. Here is the assumption: given a vector of $q + 2$ elements

$$\left(g, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}, T\right) \in G^{q+2} \tag{1}$$

it is difficult to distinguish $T = g^{(\alpha^{q+1})}$ from a random value in G. Formally speaking, for all probability polynomial time adversaries $\mathcal{A}$, the following probability is negligible:

$$\left|\Pr\left[\alpha, r \overset{R}{\leftarrow} Z_p^*;\ T_0 = g^{(\alpha^{q+1})};\ T_1 = g^r;\ z \in \{0,1\}; z' \longleftarrow \mathcal{A}\left(g, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}, T_z\right) : z = z'\right] - \frac{1}{2}\right|. \tag{2}$$

2.3. Identity-Based Proxy Reencryption. The encryption level in our paper is defined as follows: A "level 1" ciphertext is a ciphertext generated directly by the Encrypt algorithm. A "level $l + 1$" ciphertext is a reencryption result of a "level l" ciphertext by using the Reencryption algorithm. *MaxLevel* is the highest-possible ciphertext level. It is obvious that, for a single-hop IB-PRE scheme, *MaxLevel* = 2. In this paper, we deal with single-hop IB-PRE scheme, as the max level equals 2. In our scheme, the first and second level ciphertext denote the original and reencrypted ciphertext, respectively.

Definition 1 (identity-based proxy reencryption). The following algorithms describe a single-hop identity-based proxy reencryption scheme [10]:

(i) Setup(λ): the private key generator (PKG) runs setup with a security parameter λ input. This step generates the global public parameters PP and a master secret key msk.

(ii) KeyGen(msk, ID): in this step, KeyGen takes the master secret key msk and an identity ID as the input; it returns a private key sk_{ID} for identity ID.

(iii) Encrypt(ID, m): the input for this algorithm is an identity ID and a message $m \in M$ (M: message space); it generates the ciphertext C_{ID}.

(iv) RKeyGen(sk_{ID_i}, ID_i, ID_j): RKeyGen takes identities ID_i, ID_j and sk_{ID_i} and outputs the reencryption key $rk_{ID_i \longrightarrow ID_j}$.

(v) ReEncrypt($C_{ID_i}, rk_{ID_i \longrightarrow ID_j}$): a reencryption key $rk_{ID_i \longrightarrow ID_j}$ and a ciphertext C_{ID_i} corresponding to identity ID_i are the input; it returns the reencrypted ciphertext C_{ID_j}.

(vi) Decrypt(C_{ID}, sk_{ID}): given a private key sk_{ID} and a ciphertext C_{ID}, it outputs the plaintext m or it aborts with an error symbol $\perp$.

Correctness. Suppose $(PP, msk) \longleftarrow Setup(\lambda)$, $sk_{ID_i} \longleftarrow KeyGen(msk, ID_i)$, $sk_{ID_j} \longleftarrow KeyGen(msk, ID_j)$, and $rk_{ID_i \longrightarrow ID_j} \longleftarrow RKeyGen(sk_{ID_i}, ID_i, ID_j)$. The correctness of IB-PRE means that

$$\begin{aligned} &\Pr\left[Decrypt\left(C_{ID_i}, sk_{ID_i}\right) = m\right] = 1, \\ &\Pr\left[Decrypt\left(sk_{ID_j}, ReEncrypt\left(C_{ID_i}, rk_{ID_i \longrightarrow ID_j}\right)\right)\right. \\ &\quad \left. = m\right] = 1. \end{aligned} \tag{3}$$

2.4. Security Notion for Key-Private IB-PRE. We describe game-based security definition of source hiding IB-PRE in this section. Compared to the work presented in [22], our security model considers the indistinguishability of message against chosen-plaintext attack (IND-CPA) and the source hiding property of IB-PRE against chosen-plaintext attack (IND-SH-CPA).

Definition 2 (IND-CPA). A (single-use) source hiding IB-PRE scheme is IND-CPA secure if no probabilistic polynomial time (PPT) adversary $\mathscr{A}$ can win the game below with nonnegligible advantage. Next in the game, we assume λ is the security parameter and $\mathscr{B}$ is the game challenger.

(1) Setup: $\mathscr{B}$ runs the Setup(λ) algorithm to obtain the (PP, msk) and assigns PP to $\mathscr{A}$.

(2) Query phase 1:

(a) Extract(ID): run the KeyGen(msk, ID) algorithm to get sk_{ID} and return sk_{ID} to $\mathscr{A}$.

(b) RKExtract(ID_i, ID_j): run the RKeyGen(sk_{ID_i}, ID_i, ID_j) algorithm to get $rk_{ID_i \longrightarrow ID_j}$ and return $rk_{ID_i \longrightarrow ID_j}$ to $\mathscr{A}$.

(3) *Challenge.* Once $\mathscr{A}$ decides that phase 1 is finished, it outputs two equal length messages (m_0, m_1) and two challenge identities ID^*. The challenger $\mathscr{C}$ chooses a random bit $b \in \{0, 1\}$ and sends the challenge ciphertext $C^* = Encrypt(ID^*, m_b)$ to $\mathscr{A}$. The restrictions are that $\mathscr{A}$ has never made the following queries:

(i) $Extract(ID^*)$;

(ii) $RKExtract(ID^*, ID_j)$ and $Extract(ID_j)$.

(4) Query phase 2: $\mathscr{A}$ continues making queries. The queries are same as phase 1, except the followings:

(i) $Extract(ID^*)$;

(ii) $RKExtract(ID^*, ID_j)$ and $Extract(ID_j)$;

(5) Guess: $\mathscr{A}$ makes the guess b' and wins the game if $b' = b$.

We claim IB-PRE is IND-CPA secure, if the probability

$$Adv_{\mathscr{A}}^{IND-CPA}(\lambda) = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right| \tag{4}$$

is negligible for all probabilistic polynomial time adversary $\mathscr{A}$.

Next, we present the source hiding property of IB-PRE (IND-SH-CPA) and we follow the security model of [22]. IND-SH-CPA guarantees that even if an adversary knows a mailing-list address and a mailing-list member address included in the mailing-list system, the adversary cannot identify whether a source ciphertext is the source of a destination ciphertext or not. We allow an adversary to select the challenge source identities ID_0^*, ID_1^* and the challenge ciphertext ID^*. An adversary $\mathscr{A}$ is provided the *Extract* and *RKExtract* queries as in the IND-CPA game.

(1) Setup: run the Setup(λ) algorithm to get the (PP, msk) and then assign PP to $\mathscr{A}$.

(2) Query phase 1:

(a) Extract(ID): $\mathscr{A}$ runs the KeyGen(msk, ID) algorithm to get sk_{ID} and obtain sk_{ID}.

(b) RKExtract(ID_i, ID_j): $\mathscr{A}$ runs the RKeyGen(sk_{ID_i}, ID_i, ID_j) algorithm to get $rk_{ID_i \longrightarrow ID_j}$ and obtain $rk_{ID_i \longrightarrow ID_j}$.

(3) Challenge: as soon as $\mathscr{A}$ considers phase 1 is over, it outputs two identities (ID_0, ID_1), a challenge plaintext m^* and a challenge identity ID, ID not in $\{ID_0, ID_1\}$. The challenger $\mathscr{C}$ chooses a random bit $b \in \{0, 1\}$ and computes $C_{ID_b}^* = Encrypt(ID_b^*, m^*)$. Next, $\mathscr{C}$ computes $C_{ID}^* = ReEncrypt(C_{ID_b}^*, rk_{ID_b^* \longrightarrow ID})$ and sends the challenge ciphertext C_{ID}^* to $\mathscr{A}$.

(4) Query phase 2: $\mathscr{A}$ continues making queries as in the query phase 1.

(5) Guess: $\mathscr{A}$ outputs the guess b'. The adversary wins if $b' = b$.

We say that a source hiding IB-PRE scheme is IND-SH-CPA secure, if the following probability is negligible for all probabilistic polynomial time adversary $\mathcal{A}$:

$$Adv_{\mathcal{A}}^{IND-SH-CPA}(\lambda) = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right|. \quad (5)$$

Note that, unlike the IND-CPA security game, in the IND-SH-CPA security game, the adversary $\mathcal{A}$ is allowed to get the private key of the target ciphertext. The IND-SH-CPA guarantees that even if $\mathcal{A}$ can decrypt the challenge ciphertext C_{ID}^*, $\mathcal{A}$ only can obtain the following: (1) C_{ID}^* is encrypted under identity ID; (2) m^* is the plaintext, all of which however have been already known by $\mathcal{A}$.

3. Our Proposed Source Hiding IB-PRE

First, we analyze what conditions IB-PRE scheme should meet such that it has the source hiding property. Second, we describe our source hiding IB-PRE scheme and prove its IND-CPA and IND-SH-CPA security.

3.1. Impossibility Result for Source Hiding IB-PRE. Before presenting our scheme, we introduce several necessary yet not sufficient conditions that are satisfying the source hiding property.

Lemma 3. *As proven in [22], the adversary breaks the IND-SH-CPA security if he can learn to determine if destination ciphertexts are derived from the same source ciphertext or not.*

Lemma 4. *Any IB-PRE scheme, in which the ReEncrypt algorithm is deterministic, cannot satisfy source hiding.*

Proof. Suppose the *ReEncrypt* algorithm is deterministic, an adversary $\mathcal{A}$ can win the IND-SH-CPA game as below. Suppose the source ciphertext is $C_{ID_0}^*$ and $C_{ID_1}^*$ and the challenge ciphertext is C_{ID}^*. The adversary works as follows:

(1) Makes a $RKExtract(ID_1, ID)$ query and get the reencryption key $rk_{ID_1 \longrightarrow ID}$.

(2) Using the reencryption key $rk_{ID_1 \longrightarrow ID}$, run the deterministic algorithm $ReEncrypt(C_{ID_1}^*, rk_{ID_1 \longrightarrow ID}) \longrightarrow C'$.

(3) If $C' = C_{ID}^*$, it outputs 1, else returns 0.

It is not difficult to see that $\mathcal{A}$ can succeed with an overwhelming probability. □

3.2. Our Construction. Let G and G_T be bilinear group of prime order p, and g be a generator of G. Additionally, let $e : G \times G \longrightarrow G_T$ denote the bilinear map. The proposed scheme contains the following steps:

(i) Setup(λ): λ is the security parameter, and (p, g, G, G_T, e) are the bilinear map parameters. The PKG chooses random generators $g, h \in G$, random value $\alpha \in Z_p$, and a collusion resistant hash function $H : G_T \longrightarrow Z_p^*$. It sets $g_1 = g^\alpha \in G$. The PKG keeps h secret and outputs the public parameters PP. So master secrets are set as

$$PP = \left(g, g_1, e\left(g, h\right), H\right) \quad msk = \alpha. \quad (6)$$

(ii) KeyGen(msk, ID): in this step, the PKG picks a random value $r_{ID} \in Z_p$ to compute a private key for $ID \in Z_p$. It calculates $h_{ID} = (hg^{-r_{ID}})^{1/(\alpha - ID)}$ and the private key

$$sk_{ID} = \left(r_{ID}, h_{ID}\right). \quad (7)$$

If $\alpha = ID$, the PKG aborts.

(iii) Encrypt(ID, m): the input are an identity ID and a message $m \in G_T$. In this step, the sender picks a random value $s \in Z_p$ and sets

$$\begin{aligned} C_1 &= g_1^s g^{-s \cdot ID}, \\ C_2 &= g^s, \\ C_3 &= m \cdot e\left(g, h\right)^{-s}. \end{aligned} \quad (8)$$

Outputs the ciphertext $C = (C_1, C_2, C_3)$.

(iv) RKeyGen(sk_{ID_i}, ID_i, ID_j): on input identities ID_i, ID_j and the secret key sk_{ID_i}, the reencryption key $rk_{ID_i \longrightarrow ID_j}$ is generated as follows:

(1) Choose random values $\theta \in G_T$ and $s' \in Z_p$, and compute $rk_1 = (g_1^{s'} g^{-s' \cdot ID_j})$, $rk_2 = g^{s'}$, $rk_3 = \theta \cdot e(g, h)^{-s'}$.

(2) Choose a random value $\rho \in Z_p$, and set $rk_4 = r_{ID_i} \cdot H(\theta) + \rho$, $rk_5 = h_{ID_i}^{H(\theta)}$, $rk_6 = g^\rho$, and $rk_7 = e(g, h)^{H(\theta)}$.

(3) Output the reencryption key $rk_{ID_i \longrightarrow ID_j} = (rk_1, rk_2, rk_3, rk_4, rk_5, rk_6, rk_7)$.

(v) ReEncrypt($C_{ID_i}, rk_{ID_i \longrightarrow ID_j}$): on input a reencryption key $rk_{ID_i \longrightarrow ID_j} = (rk_1, rk_2, rk_3, rk_4, rk_5, rk_6, rk_7)$ and a ciphertext $C_{ID_i} = (C_1, C_2, C_3)$ under identity ID_i, the proxy proceeds as follows:

(1) Compute $C_3' = (e(C_1, rk_5) \cdot e(g, C_2)^{rk_4}) / e(C_2, rk_6)$.

(2) Choose a random value $t \in Z_p$ and compute

$$\begin{aligned} \widetilde{C_3'} &= C_3' \cdot rk_7^t, \\ \widetilde{C_3} &= C_3 \cdot e\left(g, h\right)^{-t}. \end{aligned} \quad (9)$$

(3) Choose a random value $t' \in Z_p$ and compute

$$\begin{aligned} R_1 &= rk_1 \cdot g_1^{t'} g^{-t' \cdot ID_j}, \\ R_2 &= rk_2 \cdot g^{t'}, \\ R_3 &= rk_3 \cdot e\left(g, h\right)^{-t'}. \end{aligned} \quad (10)$$

(4) Output the reencrypted ciphertext $C_{ID_i \longrightarrow DI_j} = (R_1, R_2, R_3, \widetilde{C_3'}, \widetilde{C_3})$.

(vi) Decrypt(C_{ID}, sk_{ID}):

(a) If C_{ID} is an original ciphetext, let $sk_{ID} = (r_{ID}, h_{ID})$ and $C_{ID} = (C_1, C_2, C_3)$. Compute

$$m = C_3 \cdot e\left(C_1, h_{ID}\right) \cdot e\left(g, C_2\right)^{r_{ID}}. \tag{11}$$

(b) If C_{ID} is a reencrypted ciphetext, let $C_{ID} = (R_1, R_2, R_3, \widetilde{C_3'}, \widetilde{C_3})$. Compute

$$\begin{aligned} \theta &= R_3 \cdot e\left(R_1, h_{ID}\right) \cdot e\left(g, R_2\right)^{r_{ID}}, \\ m &= \widetilde{C_3} \cdot \left(\widetilde{C_3'}\right)^{1/H(\theta)}. \end{aligned} \tag{12}$$

Correctness. The correctness of the proposed scheme is defined as follows:

(1) For an original ciphertext $C = (C_1, C_2, C_3)$, we have

$$\begin{aligned} &C_3 \cdot e\left(C_1, h_{ID}\right) \cdot e\left(g, C_2\right)^{r_{ID}} \\ &= C_3 \cdot e\left(g_1^s g^{-s \cdot ID}, \left(h g^{-r_{ID}}\right)^{1/(\alpha - ID)}\right) \cdot e\left(g, g^s\right)^{r_{ID}} \\ &= C_3 \cdot e\left(g^{s(\alpha - ID)}, \left(h g^{-r_{ID}}\right)^{1/(\alpha - ID)}\right) \cdot e\left(g, g\right)^{s r_{ID}} \\ &= C_3 \cdot e\left(g^s, h g^{-r_{ID}}\right) \cdot e\left(g, g\right)^{s r_{ID}} = m. \end{aligned} \tag{13}$$

(2) For a reencrypted ciphertext $C_{id} = (C_3, \widetilde{C_3}, rk^{(4)})$, we have

$$\begin{aligned} R_1 &= rk_1 \cdot g_1^{t'} g^{-t' \cdot ID_j} = g_1^{s'} g^{-s' \cdot ID_j} \cdot g_1^{t'} g^{-t' \cdot ID_j} \\ &= g_1^{s'+t'} g^{-(s'+t') \cdot ID_j} \triangleq g_1^{\Delta t'} g^{-\Delta t' \cdot ID_j}, \\ R_2 &= rk_2 \cdot g^{t'} = g^{s'} \cdot g^{t'} = g^{\Delta t'}, \\ R_3 &= rk_3 \cdot e\left(g, h\right)^{-t'} = \theta \cdot e\left(g, h\right)^{-s'} \cdot e\left(g, h\right)^{-t'} \\ &= \theta \cdot e\left(g, h\right)^{-\Delta t'}, \\ C_3' &= \frac{e\left(C_1, rk_5\right) \cdot e\left(g, C_2\right)^{rk_4}}{e\left(C_2, rk_6\right)} \\ &= \frac{e\left(g^{s(\alpha - ID)}, \left(h g^{-r_{ID}}\right)^{H(\theta)/(\alpha - ID)}\right) \cdot e\left(C_2, rk_6\right)}{e\left(g^s, g^\rho\right)} \\ &= \frac{e\left(g^s, \left(h g^{-r_{ID}}\right)^{H(\theta)}\right) \cdot e\left(g, g^s\right)^{r_{ID} \cdot H(\theta) + \rho}}{e\left(g^s, g^\rho\right)} \\ &= e\left(g, h\right)^{sH(\theta)}, \\ \widetilde{C_3'} &= C_3' \cdot rk_7^{\mathrm{t}} = e\left(g, h\right)^{sH(\theta)} \cdot e\left(g, h\right)^{tH(\theta)} \\ &= e\left(g, h\right)^{(s+t)H(\theta)} \triangleq e\left(g, h\right)^{\Delta t \cdot H(\theta)} \\ \widetilde{C_3} &= C_3 \cdot e\left(g, h\right)^{-t} = m \cdot e\left(g, h\right)^{-s} \cdot e\left(g, h\right)^{-t} \\ &= m \cdot e\left(g, h\right)^{-\Delta t}. \end{aligned} \tag{14}$$

Finally, we have $\widetilde{C_3} \cdot (\widetilde{C_3'})^{1/H(\theta)} = m \cdot e(g,h)^{-\Delta t} \cdot e(g,h)^{\Delta t \cdot H(\theta)/H(\theta)} = m$.

3.3. Security of Our Source Hiding IB-PRE Scheme

Theorem 5. *Our scheme is IND-CPA secure without random oracles under the q-DDHE assumption.*

Proof. Assuming there exists an adversary $\mathscr{A}$ that can break our scheme's IND-CPA security with the probability ε, we can construct an algorithm $\mathscr{B}$ that can solve the q-DDHE problem with probability ε', where

$$\varepsilon' \geq \frac{\varepsilon}{\dot{e}\left(1 + q_e\right)}. \tag{15}$$

$\mathscr{B}$ inputs a q-DDHE instance $(g, A_1 = g^\alpha, A_2 = g^{\alpha^2}, \ldots, A_q = g^{\alpha^q}, T)$ and has to distinguish $T = A_{q+1} = g^{\alpha^{q+1}}$ from a random element in G.

The approach to prove Theorem 5 follows the steps of the security proof of Gentry's scheme [25]. Note $\mathscr{B}$ maintains a list of tables that are empty initialized. Here is the list:

(i) K^{List}: it keeps the secret keys tuples (β, ID, sk_{ID}).

(ii) RK^{List}: it maintains the result of the queries to RKExtract(ID_i, ID_j) which are the tuples $(ID_i, ID_j, rk_{ID_i \longrightarrow ID_j}, flag)$. In the tuples, $flag = 1$ represents the reencryption key which is a valid one, while $flag = 0$ represents the reencryption key which is a random value.

(1) **Setup**: $\mathscr{B}$ generates a random polynomial $f(x) \in Z_p[x]$ of degree q. It sets $h = g^{f(\alpha)}$, computing h from $(g, A_1, \ldots, A_q)$. $\mathscr{B}$ also picks a collusion resistant hash function $H : G_T \longrightarrow Z_p^*$. It sends the public key $(g, A_1, e(g,h), H)$ to $\mathscr{A}$. With this assignment, the master secret key msk is α. This assignment has a distribution identical to that in the actual construction since g, α, $f(x)$, and h are uniformly random.

(2) **Query phase 1**: $\mathscr{A}$ sends a bunch of queries to $\mathscr{B}$, and $\mathscr{B}$ responds as follows:

(a) $Extract(ID)$: $\mathscr{B}$ searches K^{List}, if $(1, ID, sk_{ID})$ exists in K^{List}, then $\mathscr{B}$ obtains sk_{ID}. Otherwise, $\mathscr{B}$ generates a biased coin β so that $\Pr[\beta = 1] = \delta$ for some δ that can be determined later.

(i) If $\beta = 0$, $\mathscr{B}$ aborts and returns a random bit.

(ii) If $\beta = 1$, if $ID = \alpha$, we have that $\Pr[ID = \alpha] = 1/p$, $\mathscr{B}$ uses α to solve the q-DDHE problem. Else, let $F_{ID}(x)$ denote the $q-1$ degree polynomial $(f(x) - f(ID))/(x - ID)$. $\mathscr{B}$ returns the

private key $sk_{ID} = (r_{ID}, h_{ID}) = (f(ID), g^{F_{ID}(\alpha)})$ to the adversary and adds $(1, ID, sk_{ID})$ to K^{List}. Note that $g^{F_{ID}(\alpha)} = g^{(f(\alpha)-f(ID))/(\alpha-ID)} = (hg^{-f(ID)})^{1/(\alpha-ID)}$, which is identical to the actual construction.

(b) $RKExtract(ID_i, ID_j)$: $\mathcal{B}$ first searches whether there is a tuple $(ID_i, ID_j, rk_{ID_i \longrightarrow ID_j}, *)$ in RK^{List}. If yes, $\mathcal{B}$ returns $rk_{ID_i \longrightarrow ID_j}$ ($*$ denotes the wildcard). Otherwise, $\mathcal{B}$ proceeds as follows:

(i) If $(1, ID_i, sk_{ID_i})$ exists in K^{List}, $\mathcal{B}$ uses sk_{ID_i} to compute the reencryption key $rk_{ID_i \longrightarrow ID_j}$ by running $RKeyGen$. $\mathcal{B}$ returns $rk_{ID_i \longrightarrow ID_j}$ to $\mathcal{A}$ and adds $(ID_i, ID_j, rk_{ID_i \longrightarrow ID_j}, 1)$ to RK^{List}.

(ii) Otherwise, $\mathcal{B}$ flips a biased coin β. If $\beta = 1$, $\mathcal{B}$ queries the $Extract(ID_i)$ oracle to obtain sk_{ID_i} and then computes $rk_{ID_i \longrightarrow ID_j}$ from $RKeyGen$ algorithm. $\mathcal{B}$ returns $rk_{ID_i \longrightarrow ID_j}$ to $\mathcal{A}$ and adds $(1, ID_i, sk_{ID_i})$ and $(ID_i, ID_j, rk_{ID_i \longrightarrow ID_j}, 1)$ to K^{List} and RK^{List}, respectively. If $\beta = 0$, $\mathcal{B}$ first selects a random $\theta \in G_T$ and computes rk_1, rk_2, rk_3 as the $Encrypt$ algorithm. Next $\mathcal{B}$ computes $rk_4 = \sigma, rk_5 = \phi_1, rk_6 = \phi_2, rk_7 = e(g,h)^{H(\theta)}$ for randomly chosen $\sigma \in Z_p, \phi_1, \phi_2 \in G$. $\mathcal{B}$ forwards the reencryption key to $\mathcal{A}$ and adds $(ID_i, ID_j, rk_{ID_i \longrightarrow ID_j}, 0)$ to RK^{List}.

(3) **Challenge**: once $\mathcal{A}$ has decided that query phase 1 is over, it outputs two equal length plaintexts (m_0, m_1) and a challenge identity ID^*. If $(1, ID^*)$ exists in K^{List}, $\mathcal{B}$ outputs a random bit and aborts. Else if $\alpha = ID^*$, $\mathcal{B}$ uses α to solve the q-DDHE problem. Else $\mathcal{B}$ generates a random bit $b \in \{0,1\}$ and computes a private key (r_{ID^*}, h_{ID^*}) as in phase 1. Let $f_2(x) = x^{q+2}$ and $F_{2,ID^*}(x) = (f_2(x) - f_2(ID^*))/(x - ID^*)$; $\mathcal{B}$ sets

$$\begin{aligned} C_1^* &= g^{f_2(\alpha)-f_2(ID^*)}, \\ C_2^* &= T \cdot \prod_{i=0}^{q} g^{F_{2,ID^*,i} \cdot \alpha^i}, \\ C_3^* &= \frac{m_b}{\left(e\left(C_1^*, h_{ID^*}\right) \cdot e\left(g, C_2^*\right)^{r_{ID^*}}\right)}, \end{aligned} \tag{16}$$

where $F_{2,ID^*,i}$ is the coefficient of x^i in $F_{2,ID^*}(x)$. It sends the challenge ciphertext (C_1^*, C_2^*, C_3^*) to $\mathcal{A}$.

Note that, let $s^* = F_{2,ID^*}(\alpha)$. If $T = A_{q+1} = g^{\alpha^{q+1}}$, we have

$$C_1^* = g^{f_2(\alpha)-f_2(ID^*)} = g^{F_{2,ID^*}(\alpha)\cdot(\alpha-ID^*)} = g_1^{s^*} g^{-s^* \cdot ID^*},$$

$$\begin{aligned} C_2^* &= T \cdot \prod_{i=0}^{q} g^{F_{2,ID^*,i} \cdot \alpha^i} = g^{\alpha^{q+1}} \cdot \prod_{i=0}^{q} g^{F_{2,ID^*,i} \cdot \alpha^i} \\ &= g^{(f_2(\alpha)-f_2(ID^*))/(\alpha-ID^*)} = g^{F_{2,ID^*}(\alpha)} = g^{s^*} \end{aligned}$$

$$\begin{aligned} C_3^* &= \frac{m_b}{\left(e\left(C_1^*, h_{ID^*}\right) \cdot e\left(g, C_2^*\right)^{r_{ID^*}}\right)} \\ &= \frac{m_b}{\left(e\left(g_1^{s^*} g^{-s^* \cdot ID^*}, h_{ID^*}\right) \cdot e\left(g, g^{s^*}\right)^{r_{ID^*}}\right)} \\ &= m_b \cdot e(g,h)^{-s^*}. \end{aligned} \tag{17}$$

Thus, (C_1^*, C_2^*, C_3^*) is a valid ciphertext for (ID^*, m_b).

(4) **Query phase 2**: $\mathcal{A}$ continues querying as in the query phase 1 except for the restrictions described in the IND-CPA game.

(5) **Guess**: $\mathcal{A}$ outputs the guesse $b' \in \{0,1\}$. If $b' = b$, $\mathcal{B}$ outputs 1 meaning $T = g^{\alpha^{q+1}}$; else output 0 meaning T is a random value in G.

Probability Analysis. If $\mathcal{B}$ does not abort, $\mathcal{A}$'s view is identical to the actual scheme. Abort is defined to be the event of $\mathcal{B}'s$ aborting during the simulation of $Extract$ query. Let q_e denote the total number of $Extract$ queries; we have $\Pr[\neg Abort] \geq \delta^{q_e} \cdot ((p-1)/p)^{q_e} \triangleq \xi^{q_e} \geq \xi^{q_e}(1-\xi)$, which is maximized at $\delta_{opt} = q_e/(1+q_e)$. Using δ_{opt}, the probability $\Pr[\neg Abort]$ is at least $1/\dot{e}(1+q_e)$, where $\dot{e}$ is the base of the nature logarithm. Therefor, we have $\varepsilon' \geq \varepsilon/\dot{e}(1+q_e)$.

This completes the proof of Theorem 5. □

Theorem 6. *Our proposed scheme is IND-SH-CPA secure in the information theoretic sense.*

Proof. Since a source identity ID_i is not included in a destination ciphertext, Theorem 6 is clearly satisfied. $(R_1, R_2, R_3, \widetilde{C_3'}, \widetilde{C_3})$ as $R_1 = g_1^{\Delta t'} g^{-\Delta t' \cdot ID_j}$, $R_2 = g^{\Delta t'}$, $R_3 = \theta \cdot e(g,h)^{-\Delta t'}$, $\widetilde{C_3'} = e(g,h)^{\Delta t \cdot H(\theta)}$, and $\widetilde{C_3} = m \cdot e(g,h)^{-\Delta t}$, where ID_j is a destination ciphertext, namely, a part of source ciphertext C_3 is randomized using a random value t. More precisely, for $C_{ID_j} = (R_1, R_2, R_3, \widetilde{C_3'}, \widetilde{C_3})$ and all identity ID, there exists a ciphertext $C_{ID} = (g_1^s g^{-s \cdot ID}, g^s, m \cdot e(g,h)^{-s})$ which can be a source ciphertext of C_{ID_j}.

This completes the proof of Theorem 6. □

4. Performance and Comparison

4.1. Efficiency Theoretical Analysis. To compare the performance of our scheme, we choose the existing source hiding IB-PRE scheme [22] as the base. We make the comparison in the aspect of the public/private key size, reencryption key size, level 1/level 2 ciphertext size, reencryption key generation cost, reencryption cost, and security model. Table 1 illustrates the detailed comparison. To construct a fair comparison, we choose Emura, Miyaji, and Omote's first scheme denotes EMO 1 scheme [22], which is also CPA secure with source hiding. Let c_e, c_p represent the computational cost of an exponentiation and a pairing cost, respectively, $|Z_p|$, $|G|$, $|G_T|$ denote the bit-length of an element in Z_p, G, G_T, respectively, and $|H|$ denotes the size of a hash function.

Table 1: Efficiency and security comparison.

Schemes	EMO scheme [22]	Our IB-PRE scheme
Public/Private key size	$2\|G\| + 2\|H\| /\|Z_p\|$	$2\|G\| + \|G_T\| + \|H\| /\|Z_p\|$
Re-encryption key size	$2\|G\| + \|G_T\|$	$4\|G\| + 2\|G_T\| + \|Z_p\|$
Level 1/Level 2 ciphertext size	$\|G\| + \|G_T\| /2\|G\| + 2\|G_T\|$	$2\|G\| + \|G_T\| /2\|G\| + 3\|G_T\|$
Rekey generation/ Re-encryption cost	$3c_e + c_p /4c_e + 3c_p$	$7c_e /7c_e + 3c_p$
Without RO?	×	✓
Collusion resistant	×	✓

Table 2: Execute time comparison.

Algorithms	KeyGen (ms)	Enc (ms)	RKenGen (ms)	ReEnc (ms)	Dec(Or) (ms)	Dec(Re) (ms)
scheme [22]	3.279	4.662	6.441	4.971	5.082	6.506
Our scheme	3.795	5.103	6.061	9.017	5.602	7.032

From Table 1, we found that, although the ciphertext size of our scheme is a little larger than the scheme of [22] in terms of the computational cost. However, the computational cost is the same order of magnitude. Most of important, our scheme is collusion resistant and without relying on random oracle.

4.2. Execute Time. Now we compare the proposed scheme with the existing source hiding IB-PRE scheme [22] regarding the execute time. For the scheme implementation, we use the Pairing Based Cryptography Library [26] to calculate the implementation time. Our Hardware is Intel(R) Core(TM) i5-8250U CPU @ 1.60GHZ 8GB RAM. The operation system is Linux Mint 18.1 Serena and programming language is GO 1.9. The elliptic curve $Y^2 = X^3 + X$ and the group order is 160 bits which are selected for the experiment. In our experiment we run each experiment for 20 times to obtain the average execution time.

From Table 2, it is observable that the execution time of *KeyGen*, *Enc*, *RKeyGen*, *ReEnc*, *Dec*(*Or*), and *Dec*(*Or*) of our scheme is a little more than scheme [22]. This coincides with the theoretical analysis.

5. Conclusions

In this paper, we introduced a new source hiding identity-based proxy reencryption scheme (SHIB-PRE) which is proposed to support a gateway of the wireless network to directly convert a user's encrypted data (encrypted pollution data) to a new user's encrypted data without exposing the underlying plaintext data during the whole sharing phase. Additionally, our SHIB-PRE scheme addresses the open problems left by Emura, Miyaji, and Omote [22] by presenting collusion resistant, source hiding, and against chosen ciphertext-plaintext attack secure in the standard model. Still, interesting questions are remained to be resolved and can be our future work, such as the following:

CCA-Secure. Designing a source hiding IB-PRE scheme that is chosen ciphertext secure is necessary. The technique described in [27] might be the potential approach to achieve CCA-secure.

Key-Private IB-PRE. The property of source hiding protects the source identity from a destination ciphertext. It will be challenging to design a key-private IB-PRE, in which a source identity and a destination identity are not disclosed from a reencryption key. The technique presented in [28] could be the potential approach to achieve a key-private IB-PRE scheme.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that the funding in Acknowledgments section did not lead to any conflicts of interest regarding the publication of this manuscript. Also, there is no any other conflicts of interest in the manuscript.

Acknowledgments

Chunpeng Ge is supported by the National Natural Science Foundation of China (no. 61702236) and Changzhou Sci&Tech Program (no. CJ20179027), Jinyue Xia is partially supported by the National Natural Science Foundation of China (no. 6127208361300236), and Hongwei Li is partially supported by the National Natural Science Foundation of China (no. 61702216).

References

[1] J. Cui, Y. Zhang, Z. Cai, A. Liu, and Y. Li, "Secring display path for security-sensitive applications on mobile devices," *Computers, Materials & Continua*, vol. 55, no. 1, pp. 17–35, 2018.

[2] A. Pradeep, S. Mridula, and P. Mohanan, "High security identity tags using spiral resonators," *Computers, Materials and Continua*, vol. 52, no. 3, pp. 185–195, 2016.

[3] IBM, "Ibm smart cloud," http://ibm.com/cloudcomputing/.

[4] Amazon, "Amazon web services (aws)," http://aws.amazon.com.

[5] Z. Xiangyang, D. Hua, Y. Xun, Y. Geng, and L. Xiao, "MUSE: An Efficient and Accurate Verifiable Privacy-Preserving Multi-keyword Text Search over Encrypted Cloud Data," *Security and Communication Networks*, vol. 2017, 2017.

[6] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, "Adaptive fractional-Pixel motion estimation skipped algorithm for efficient HEVC motion estimation," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 14, no. 1, pp. 1–19, 2018.

[7] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology—EUROCRYPT '98 (Espoo)*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 127–144, Springer, Berlin, Germany, 1998.

[8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[9] Y. Ren, J. Shen, D. Liu, J. Wang, and J.-U. Kim, "Evidential quality preserving of electronic record in cloud storage," *Journal of Internet Technology*, vol. 17, no. 6, pp. 1125–1132, 2016.

[10] J. Katz and M. Yung, "Identity-based proxy re-encryption," in *Proceedings of the nternational Conference on Applied Cryptography and Network Security*, pp. 288–306, 2007.

[11] C. K. Chu and W. G. Tzeng, "Identity-based proxy re-encryption without random oracles," in *International Conference on Information Security*, pp. 189–202, 2007.

[12] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles," in *Information Security and Cryptology – ICISC 2012*, vol. 7839 of *Lecture Notes in Computer Science*, pp. 231–246, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[13] C. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy," *Computer Standards & Interfaces*, vol. 52, pp. 1–9, 2017.

[14] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)*, pp. 276–286, March 2009.

[15] S. Luo, J. Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *Information and Communications Security*, M. Soriano, S. Qing, and J. López, Eds., vol. 6476 of *Lecture Notes in Computer Science*, pp. 401–415, Springer, Berlin, Germany, 2010.

[16] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems, INCoS 2013*, pp. 552–559, China, September 2013.

[17] N. Helil and K. Rahman, "CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy," *Security and Communication Networks*, vol. 2017, 2017.

[18] Z. Liu and D. S. Wong, "Practical ciphertext-policy attribute-based encryption: traitor tracing, revocation, and large universe," in *Applied Cryptography and Network Security*, vol. 9092 of *Lecture Notes in Comput. Sci.*, pp. 127–146, Springer, [Cham], 2015.

[19] C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," *The Computer Journal*, vol. 59, no. 7, pp. 970–982, 2016.

[20] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," *Designs, Codes and Cryptography. An International Journal*, vol. 86, no. 11, pp. 2587–2603, 2018.

[21] K. Liang, M. H. Au, J. K. Liu et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1667–1680, 2014.

[22] K. Emura, A. Miyaji, and K. Omote, "An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system," *European Public Key Infrastructure Workshop*, vol. 6711, pp. 77–92, 2010.

[23] C. Ran, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in *Proceedings of ACM Symposium on Theory of Computing*, pp. 209–218, 1998.

[24] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[25] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in cryptology—EUROCRYPT*, vol. 4004 of *Lecture Notes in Comput. Sci.*, pp. 445–464, Springer, Berlin, 2006.

[26] "Library P. Pbc library," http://github.com/Nik-U/pbc.

[27] C. Ran, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 207–222, 2004.

[28] J. Shao, P. Liu, and Y. Zhou, "Achieving key privacy without losing CCA security in proxy re-encryption," *The Journal of Systems and Software*, vol. 85, no. 3, pp. 655–665, 2012.