An ID-based Broadcast Encryption Scheme for Cloud-network Integration in Smart Grid

Shufen Niu, Lizhi Fang*, Mi Song, Fei Yu and Song Han
College of Computer Science and Engineering, Northwest Normal University
Lanzhou 730070, China
[e-mail: sfniu76@nwnu.edu.cn, 1439902640@qq.com, 1744391811@qq.com, yf_1997163@163.com, 565904313@qq.com]
*Corresponding author: Lizhi Fang

Received April 29, 2021; revised July 27, 2021; accepted August 29, 2021; published September 30, 2021

Abstract

The rapid growth of data has successfully promoted the development of modern information and communication technologies, which are used to process data generated by public urban departments and citizens in modern cities. In specific application areas where the ciphertext of messages generated by different users' needs to be transmitted, the concept of broadcast encryption is important. It can not only improve the transmission efficiency but also reduce the cost. However, the existing schemes cannot entirely ensure the privacy of receivers and dynamically adjust the user authorization. To mitigate these deficiencies, we propose an efficient, secure identity-based broadcast encryption scheme that achieves direct revocation and receiver anonymity, along with the analysis of smart grid solutions. Moreover, we constructed a security model to ensure wireless data transmission under cloud computing and internet of things integrated devices. The achieved results reveal that the proposed scheme is semantically secure in the random oracle model. The performance of the proposed scheme is evaluated through theoretical analysis and numerical experiments.

Keywords: Smart grid, IoT, Identity-based, Broadcast encryption, Privacy-preserving

http://doi.org/10.3837/tiis.2021.09.015 **ISSN : 1976-7277**

1. Introduction

With the rapid growth of the world population, a series of problems have appeared in urban governance. Providing some public services by the government is necessary to enhance the quality of life of citizens. A practical and safe monitoring network must be established to ensure sensitive information, such as water, electricity, and transportation. Traditional techniques and management methods are difficult to address effectively. Therefore, utilizing emerging information and communication technologies is essential to address the management of urbanization. In this context, some outstanding scholars have proposed the concept of smart cities [1,2]. For example, Zhang et al. [3] introduced the deficiencies in applying the internet of things (IoT) to smart homes, smart communities, smart grids, and public infrastructure scenarios. Ejaz et al. [4] used two practical examples to summarize the current energy management problems of IoT universities in smart cities. Specifically, the scheme in [4] considers how to effectively reduce energy consumption in the smart home, smart education, smart health, intelligent traffic systems (ITS) and smart industry application fields.

Smart grid is one of the application areas of smart cities, and it is a favorable trend for the development of power grid technology. At present, traditional power grids must rely on smart technology to achieve security information defense capabilities and self-healing capabilities to realize the development and transmission of clean energy while resisting natural disasters and external interference. What is more, smart technology can reduce costs and is cost-effective [5]. However, conventional research has shown that information cannot be transmitted effectively due to the backwardness of many devices and technical deficiencies [6,7].

A possible scheme requires the smart power control center to encrypt and broadcast the ciphertext to the user for transmitting user electricity information efficiently and securely. Broadcast encryption technology allows broadcast servers to share messages with a group of receivers. However, many existing broadcast encryption schemes still have problems and challenges with smart grid data transmission. For instance, they are unable to achieve receiver anonymity. Furthermore, if the receivers leave the power system or malicious users, we must guarantee that direct revocation is implemented under data access control to adapt to the characteristics of the smart grid for transmitting lightweight files in the Internet of Things environment. Therefore, we also consider how to revoke the receivers of the specified set from the ciphertext generated. Our scheme's main contributions are summarized as follows:

- We propose an efficient and privacy-preserving broadcast encryption scheme. Broadcast encryption is employed to guarantee transmission efficiency among broadcasters and users; Lagrange interpolation technology realizes the properties of receiver anonymity.
- The proposed scheme model combines smart grid application scenarios in smart cities for power data sharing. From the perspective of smart city users, leaving the system will cause information updates and other issues. We use the direct revocation method, which allows the user's access privileges to be dynamically adjusted.
- We reduced expensive bilinear pairing operations to achieve more lightweight broadcasts and provided a comprehensive security proof and performance analysis of our scheme. The results showed that the efficiency and security of our scheme surpass that of existing schemes, and it is more suitable for practical applications.

In the following two sections, we will briefly review related works and the preliminaries, respectively. The proposed scheme and security proof are respectively presented in sections 4 and 5. In section 6, we present the performance evaluation. The paper is summarized in the last section.

2. Related works

At present, the emergence of sensor technology has a tremendous impact on conventional the grid, which collects detailed power information through sensor devices. Fortunately, sensor networks also provide technical support for power grid state analysis, making the traditional power grid smart. To ensure the security and privacy of information, Yasir Saleem et al. Saleem et al, 2019 [8] discussed power energy waste and data transmission security, and integrated internet of things devices to achieve the generation, distribution, transmission, and use of power data.

However, electricity consumption data may be tampered with or illegally accessed during transmission, which brings huge security risks to the smart grid environment. Only if the ciphertext and user identity satisfy the privacy-preserving properties, can the corresponding power information be safely transmitted. Therefore, smart grid access control schemes are emerging one after another nowadays. Fiat et al. [9] proposed the broadcast encryption technology in 1993, which allows the central broadcasting station to broadcast the ciphertext to any set of receivers while minimizing the transmission associated with key management. Privacy is a crucial issue in the broadcast environment. To satisfy the security and anonymity requirements of the broadcaster and receiver's communication, the schemes in [10,11,12] use broadcast encryption technology to protect the privacy and confidentiality of information in a multi-receiver environment. However, the aforesaid scheme cannot achieve the complication of malevolent and revoked receiver's adjustment access privileges. Significations, the schemes in [10] introduced Lagrange interpolation and embed user identity in ciphertext to realize receiver anonymity.

Direct revocation is an essential technique for standard broadcast encryption scheme. It is used to adjust authorization between multiple receivers such that only receivers within a receiver set specified by the smart power control center can decrypt the ciphertext. A quantity of work with direct revocation for the area has been proposed. For instance, Jia et al. [13] applied the constant-size ciphertext and private key property of revocation to a broadcast encryption scheme. To improve efficiency, Zhu et al. [14] constructed a mechanism to support designation and revocation and introduced dual-modes. In [15], Li et al. present a new broadcast encryption scheme for prime-order bilinear groups which achieves revocation. However, these works are not aimed at solving receiver anonymity.

To the best of our investigation, Lai et al. [16,17,18,19] proposed broadcast encryption based on anonymous identities in 2016 and 2017, allowing the data owner to effectively broadcast ciphertext to a multi-receiver. These schemes support the direct revocation of the user's identity, focusing on data access control, where the data owner sends ciphertexts to authorize users to realize the sharing of ciphertexts. However, these three schemes achieve identity anonymity between receivers, but a large amount of transmission and computation results in low computation efficiency. Nonetheless, in 2019, Wang et al. [20] presented an IBDE broadcast scheme and devised a secure economic data sharing protocol. The scheme is semi-adaptively semantically secure, but it does not guarantee the construction of public-key broadcast encryption by Guo et al [21]. Constructing public-key broadcast encryption could not realize privacy-preserving and authorization revocation.

3. Preliminaries

In this section, we give the smart grid solution and security goals. **Table 1** provides the descriptions of the key symbols used in the proposed scheme.

3.1 Smart grid solution

We consider the smart grid solution, as shown in **Fig. 1**. Following the smart grid solution in the IoT environment, the primary technologies for each layer are as follows:

perception layer. The perception layer is at the bottom. It mainly includes smart meters, RFID readers, sensors, monitors, M2M and other smart devices for sensing and identifying objects. Collect power consumption data of the users in the system.

network layer. The middle layer uses wired and wireless networks as the nerve center. This layer, called the network layer, realizes the broadcast communication transmission of events on the Internet. It mainly uses WLAN, 3G/4G network, LMDS and other internet technologies to achieve interconnection communication between the smart power control center and users.

platform layer. The middle platform layer has an aggregation switch that inherits user information gathered by the perception layer and supports the IoT infrastructure. In the integrated operating environment of the IoT, the aggregation switch can not only store, calculate, and distribute user data but also manage the user registration privileges in the system.

application layer. The top-layer in the entire architecture of information processing is the application layer. The smart power control center at the application layer can perform internal power dispatch, comprehensive evaluation, and regular maintenance of internal service equipment. For external services, whether government agencies, residential areas, schools, industrial areas or other users, it can provide a smart, accurate and secure power supply.

In many smart grid scenes, each smart meter in the perception layer is equipped with implanted sensor chips. The smart power control center could do real-time remote monitoring of the user's power conditions by collecting the power data (i.e., power consumption, power use time and instantaneous peak power) through wireless sensor nodes.

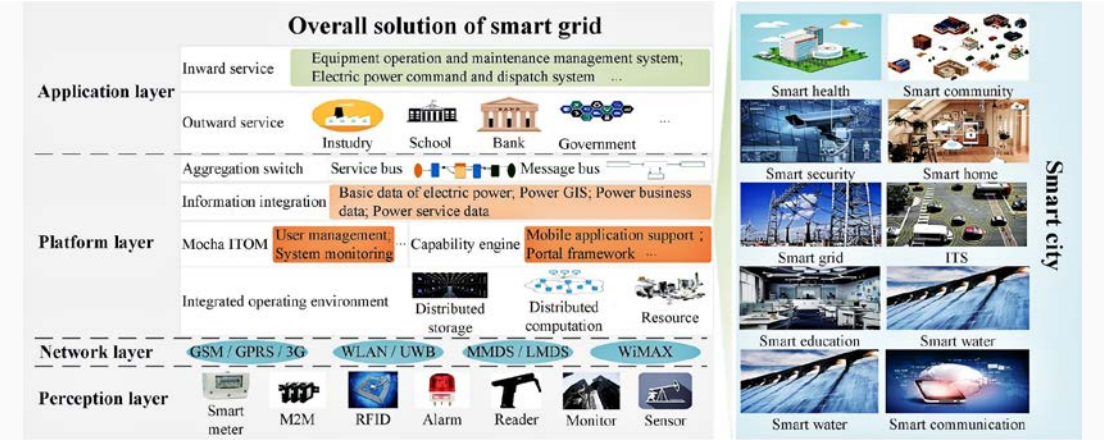


Fig. 1. Example application domains in a smart city

The information gathered by the Internet is aggregated to the sink node in the platform layer directly. Then, the control devices distribute, store, and compute the power information in the integrated operating environment, respectively. Finally, apply the encapsulated information to internal services for users to access.

3.2 Security Notions

Based on the scheme in [22], our scheme defines four security models, respectively: identity-based chosen plaintext attack (IND-ID-CPA) security, anonymous identity-based chosen plaintext attack (ANON-ID-CPA) security, revocable identity-based chosen plaintext attack

(IND-rID-CPA) security, and revocable anonymous identity-based chosen plaintext attack (selective ANON-rID-CPA) security. The four security goals by probability polynomial-time between adversary A and challenger C game to define.

Game 1. IND-ID-CPA security.

This game, under the IND-ID-CPA security model, is played between adversary A and challenger C. The security model is defined as follows:

Setup: Challenger C establishes the algorithm, inputs the security parameter λ, outputs mpk, and keeps msk.

Phase 1: Adversary A can issue private key queries. When receiving private queries about the identity set ID_i, the challenger C generates d_{ID_i} and returns it.

Challenge: Adversary A after the decision **Phase 1** is over. Without the restriction of initiating a private key query for any $ID_i \in S^*$, adversary A outputs two messages of different lengths; M_0, M_1 and the challenge set $S^* = (ID_1, ID_2, \mathrm{L}, ID_n)$. Challenger C picks a bit $b \in \{0,1\}$, and outputs the challenge ciphertext CT^* for M_b under S^*.

Table 1. Notations and Descriptions

Notation	Description
PKG	Key Generation Center
λ	Security parameter
P	Generator of G
H , H_1 , H_2 , H_3	Secure hash function
mpk	System public key
msk	Master key
d_{ID}	User private key
S	User identity set
R	Revocation identity set
M	Message
$i = 1, \mathrm{L}, n$	The number of users
r_1 , k_1 , k_2	Random number
CT	Ciphertext
CT'	Ciphertext after revocation

Phase 2: Subject to the above **Challenge**, A issues more private key queries.

Guess: If $b = b'$, and adversary A outputs $b' \in \{0,1\}$ and wins the game, we call the adversary game IND-ID-CPA adversary and wins the game with probability adversary $Adv^{A,M}_{IND-ID-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|$.

Definition 1. If the IND-ID-CPA adversary's advantage $Adv^{A,M}_{IND-ID-CPA}(\lambda)$ in **Game 1** is negligible in any polynomial time, the proposed ID-based broadcast encryption scheme for cloud network integration is IND-ID-CPA security.

Game 2. ANON-ID-CPA security.

The working principle of this security model is as follows: **Setup**, **Phase 1**, and **Phase 2** are the same as in **Game 1**.

Challenge: Adversary A generates M^*, two different sets $S_0 = \{ID_{0,1}, ID_{0,2}, \ldots, ID_{0,n}\}$ and $S_1 = \{ID_{1,1}, ID_{1,2}, \ldots, ID_{1,n}\}$ for any $ID_i \in S_0 \vee S_1 = (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$. Challenger C outputs CT^* for M^* under S_b.

Guess: If $b = b'$, and adversary A outputs $b' \in \{0,1\}$ and wins the game, we call the adversary game ANON-rID-CPA adversary and wins the game with probability $Adv^{A,M}_{ANON-ID-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|$.

Definition 2. If the ANON-ID-CPA adversary's advantage $Adv^{A,M}_{ANON-ID-CPA}(\lambda)$ in **Game 2** is negligible in any polynomial time, the proposed ID-based broadcast encryption scheme for cloud network integration is ANON-ID-CPA security.

Game 3. IND-rID-CPA security.

The IND-rID-CPA security model is defined as follows: **Setup**, **Phase 1**, and **Phase 2** are the same as in **Game 1**.

Challenge: Without the restriction of issuing private key queries, adversary A generates $R^* = \{ID_{l_1}, ID_{l_2}, \ldots, ID_{l_t}\}$ for any $ID_i \in S^* \setminus R^*$. Challenger C executes **Encrypt** and **Revoke** algorithms, generates CT^* for message M_b under S^* and R^*.

Guess: If $b = b'$, and adversary A outputs $b' \in \{0,1\}$ and wins the game, we call the adversary game IND-rID-CPA adversary and wins the game with probability $Adv^{A,M}_{IND-rID-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|$.

Definition 3. If the IND-rID-CPA adversary's advantage $Adv^{A,M}_{IND-rID-CPA}(\lambda)$ in **Game 3** is negligible in any polynomial time, the proposed ID-based broadcast encryption scheme for cloud network integration is IND-rID-CPA security.

Game 4. Selective ANON-rID-CPA security.

Given two revocation sets of different lengths, **Setup** and **Phase 1** are the same as in **Game 1**.

Init: Adversary A outputs $R_0 = \{ID_{0,1}, ID_{0,2}, \ldots, ID_{0,t}\}$ and $R_1 = \{ID_{1,1}, ID_{1,2}, \ldots, ID_{1,t}\}$.

Challenge: A outputs M^* and broadcasts set $S^* = (ID_1, ID_2, \ldots, ID_n)$. Challenger C outputs CT^* for M^* under S^* and R_b.

Phase 2: Adversary A initiates more private key queries to $ID_i \notin R_0 \vee R_1$.

Guess: If $b = b'$, and adversary A outputs $b' \in \{0,1\}$ and wins the game, we call the adversary game ANON-rID-CPA adversary and wins the game with probability $Adv^{A,M}_{ANON-rID-CPA}(\lambda) = \left| \Pr[b = b'] - \frac{1}{2} \right|$.

Definition 4. If the ANON-rID-CPA adversary's advantage $Adv^{A,M}_{ANON-rID-CPA}(\lambda)$ in **Game 3** is negligible in any polynomial time, the proposed ID-based broadcast encryption scheme for cloud network integration is selective ANON-rID-CPA security.

4. System construction

In this section, we introduce the application scenarios and basic construction of our scheme. The purpose of our scheme is to achieve the security of data transmission between smart grid

and residential users in the cloud-network integration environment.

4.1 Basic construction of the scheme

The smart grid is a typical application scenario for broadcast encryption schemes in smart cities. In the smart grid, the data in transit (that is, between smart devices and the smart power control center) is encrypted to ensure the users' privacy.

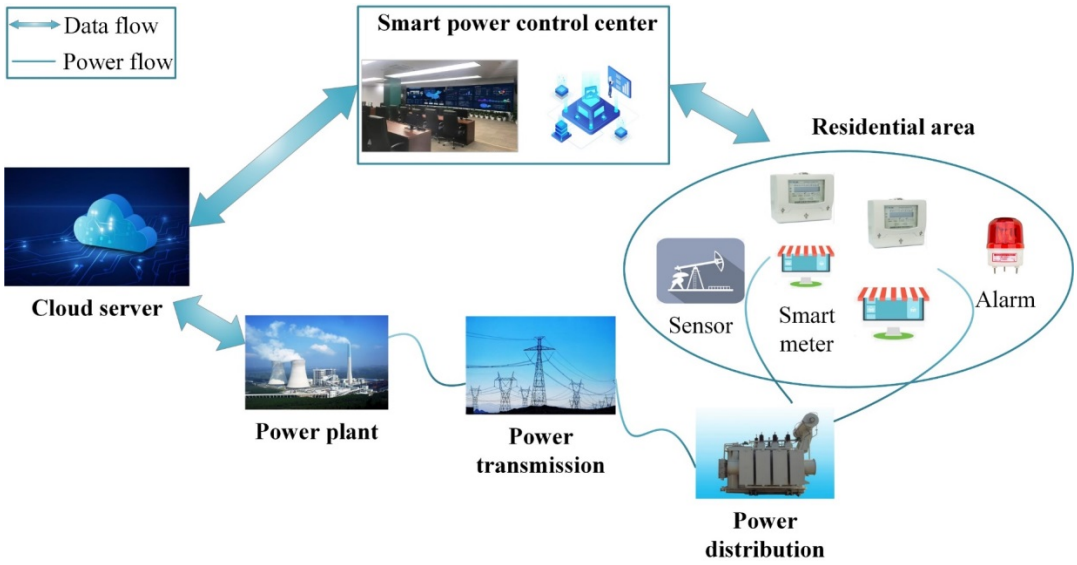


Fig. 2. A typical application scenario in smart grid

As shown in **Fig. 2**, our scheme is suitable for one-to-many ciphertext broadcast scenarios. The cloud-network model mainly includes five entities: private key generator (PKG), smart power control center, cloud server, smart device (smart meter), and data user. We assume the PKG is fully trusted and the cloud server is semi-trusted, which signifies that the cloud server follows the scheme, but is curious about the ciphertext. The PKG generates private keys for the smart power control center and receivers. Then, the smart power control center encrypts messages and transmits the original ciphertext to the cloud server. The cloud server transmits the ciphertext to the power plant and performs power transmission and computation through the network. Finally, it distributes the power ciphertext to users in residential areas. In the entire power transmission process, however, the user who can receive the key has the privileges to use the smart power service and access the ciphertext. The scheme includes the following five algorithms:

Setup $\left(1^{\lambda}\right) \rightarrow mpk, msk$: It is executed by the PKG that inputs security parameter λ :

- The PKG randomly selects a bilinear group $BG = \left(G, G_T, e, p\right)$, with generator $P \in G$. Then, it chooses a random integer $s \in Z_p$, and computes public key $P_{pub} = sP$;
- It picks four collision-resistant hash functions:

$$H : \{0,1\}^* \rightarrow Z_p,\ H_1 : \{0,1\}^* \rightarrow G,\ H_2 : G_T \times \{0,1\}^* \rightarrow G \text{ and } H_3 : G_T \times \{0,1\}^* \rightarrow G;$$

- Finally, the PKG outputs $mpk = \left(BG, P, P_{pub}, H, H_1, H_2, H_3\right)$ and $msk = s$.

Keygen $\left(mpk, msk, ID\right) \rightarrow d_{ID}$: On receiving $\left(mpk, msk\right)$ and user identity $ID \in \{0,1\}^*$, the PKG executes the algorithm to compute $d_{ID} = sH_1\left(ID\right)$ for the user.

Encrypt $(mpk, M, S) \to CT$: The broadcaster, also known as the smart power control center, inputs mpk , receiver set $S = (ID_1, ID_2, \text{L}\ , ID_n)$ and $M \in G$ to be shared with the user message. It executes the following steps to generate broadcast ciphertext CT . The encryption phase model is shown in **Fig. 3**.

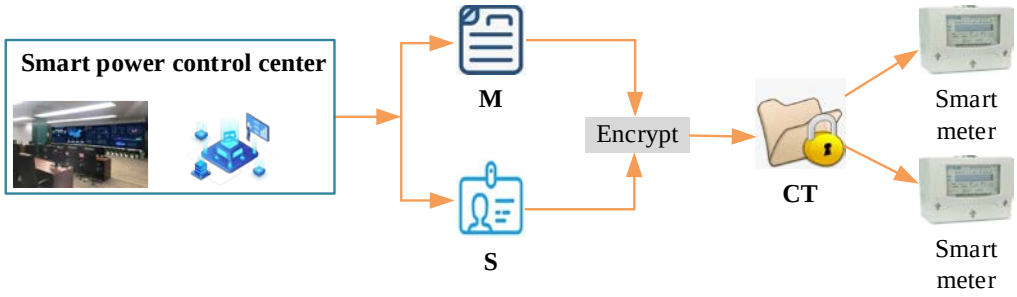


Fig. 3. Data encrypt

- It first extracts the function H from the mpk , computes $x_i = H(ID_i)$ for $i(i = 1, 2, \text{L}\ , n)$, and constructs a polynomial function $f_i(x) = \sum_{j=0}^{n-1} a_{i,j} x^j \bmod p$;
- It then randomly chooses two secret integers $r_1 \in Z_p$ and $k_1 \in G$ to compute $A_i = k_1 + H_3\left(e\left(H_1(ID_i), P_{pub}\right)^{r_1}, ID_i\right), i \in [1, n]$, we have $f_i(x_i) = 1$ and $f_i(x_j) = 0$ for $i \neq j$;
- It computes $C_0 = k_1 + M$, $C_1 = r_1 P$ and $u_i = \sum_{j=1}^{n} a_{j,i-1} A_j$, $i = 1, 2, \text{L}\ , n$;
- It then sets $Hdr = (\{u_i : 1 \le i \le n\}, C_1)$ as broadcast-header;
- It generates the broadcast body ciphertext $C_M = (C_0, A_i : 1 \le n \le i)$;
- Finally, it broadcasts $CT = (Hdr, C_M)$ to the cloud server to be stored in the smart meter.

Revoke $(mpk, R, CT) \to CT'$: Takes the mpk revocation identity set R and broadcasts the ciphertext $CT = (Hdr, C_M)$ as input. The received original ciphertext CT is re-encrypted according to the identity of the revoked user to obtain the revoked ciphertext CT' . In this process, the cloud server performs the algorithm and uses Lagrange interpolation to hide the receiver's identity, but it cannot obtain any user identity or sensitive information from the ciphertext.

- If revocation identity set $R = \varnothing$, then the cloud server sets $CT' = CT$. Otherwise, it randomly selects an integer $k_2 \in G$ to compute $C_0' = k_2 + C_0$ and $x_i = H(ID_i)$ for $ID_i \in R$. It then constructs polynomial the function $g(x) = \prod_{i=1}^{t} (x - x_i) = \sum_{i=1}^{t} b_i x^{i-1} \bmod p$;
- For any $i = 1, 2, \text{L}\ , n$, it computes $T_i = g(x_i)^{-1} b_i k_2$, $b_i = 0$, where $i = t+1, t+2, \text{L}\ , n-1$;
- It sets $Hdr = (\{T_i : 1 \le i \le n\})$ as broadcast-header after revocation;
- It then generates the broadcast body ciphertext $C_M' = (R, C_0')$;
- Finally, it broadcasts the ciphertext $CT' = (Hdr, C_M')$ to the user and stores it in the smart meter.

Decrypt $(mpk, CT', ID_i, d_{ID}) \rightarrow M$: Taking the mpk , ciphertext after revocation CT' , receiver's identity ID_i , and privacy key d_{ID} as input, the user executes the decryption algorithm to obtain the plaintext M . The revocation phase and the decryption phase model are shown in **Fig. 4**.

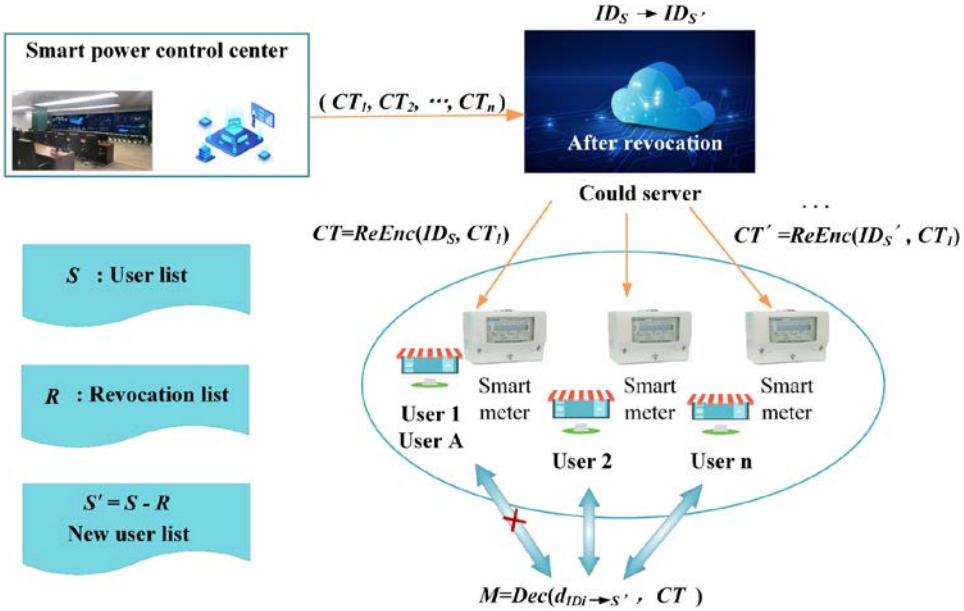


Fig. 4. ID revoke and Data decrypt

- It extracts the functions H from the mpk , computes $x_i = H(ID_i)$, $i = 1,2,\ldots,n$;
- It parses out $u = u_1 + x_i u_2 + x_i^2 u_3 + \ldots + x_i^{n-1} u_n$ from $\{u_i : 1 \le i \le n\}$;
- It then obtains $k_1' = u - H_3\left(e\left(C_1, d_{ID_i}\right), ID_i\right)$ and $k_2' = T_1 + x_i T_2 + x_i^2 T_3 + \ldots + x_i^{t-1} T_t$;

Finally, it recovers message $M = C_0' - k_1' - k_2'$. If the identity satisfies $ID_i \in S$ and $ID_i \notin R$, where $k_1' = k_1$, $k_2' = k_2$, the ciphertext is decrypted to obtain the correct plaintext.

In the definition of an encryption algorithm, the size of the revocation number $t < n$ depends on the real situation of the application. If $t = 0$, the data owner does not allow the server to revoke any user's identity. $t = n$ indicates that the data owner allows the server to revoke any identity status in the set.

***Correctness*:** We give the correctness of our proposed scheme as follows:

For each $ID_i \in S$, after obtaining x_i by using its private key, we compute

$$\begin{aligned} u &= u_1 + x_i u_2 + x_i^2 u_3 + \ldots + x_i^{n-1} u_n \\ &= \left(a_{1,0} + a_{1,1} x_i + a_{1,2} x_i^2 + \ldots + a_{1,n-1} x_i^{n-1}\right) A_1 \\ &\quad + \left(a_{2,0} + a_{2,1} x_i + a_{2,2} x_i^2 + \ldots + a_{2,n-1} x_i^{n-1}\right) A_2 + , \\ &\quad \ldots + \left(a_{n,0} + a_{n,1} x_i + a_{n,2} x_i^2 \ldots + a_{n,n-1} x_i^{n-1}\right) A_n \\ &= f_1(x_i) A_1 + f_2(x_i) A_2 + \ldots + f_n(x_i) A_n = A_i \end{aligned}$$

Then, we compute k_1' as

$$k_1' = u - H_3\left(e\left(C_1, d_{ID_i}\right), ID_i\right) = k_1 + H_3\left(e\left(sH_1(ID_i), P\right)^{r_1}, ID_i\right) - H_3\left(e\left(P, sH_1(ID_i)^{r_1}, ID_i\right)\right) = k_1 ,$$

For any $ID_i \in S$ and $ID_i \notin R$, $g(x_i) \neq 0$ and we obtain k_2' as

$$k_2' = T_1 + x_i T_2 + x_i^2 T_3 + \mathsf{L} + x_i^{t-1} T_t = g(x_i)^{-1} k_2 g(x_i) = k_2,$$

After recovering k_1' and k_2', we obtain the message as

$$C_0' - k_1' - k_2' = k_2' + C_0 - k_1' - k_2' = k_1 + M - k_1' = M.$$

5. Security proof

In this section, we give the security proof of the proposed scheme.

Definition 5. BDH [23]. Let G and G_T be multiplicative cyclic groups of prime order p and P be the generators of G and the bilinear map $e: G \times G \to G_T$. Given (P, aP, bP, cP) for unknown $a,b,c \in Z_p$, we compute $e(P,P)^{abc} \in G_T$. Adversary A has advantage ε in solving the BDH problem if $Pr\left[A(P, aP, bP, cP) = e(P,P)^{abc}\right] \geq \varepsilon$.

Theorem 1. Defines functions H and H_3. If the BDH assumption holds, A attacks our scheme with advantage ε, the algorithm B solves the BDH problem with advantage $\varepsilon' \geq \varepsilon \cdot \left(e \cdot n \cdot q_E \cdot q_{H_3}\right)^{-1}$. n is the number of broadcast identities, q_E is the number of queries to the private key and q_{H_3} is the number of queries to the hash function H_3.

Proof. If there is IND-ID-CPA adversary, it will attack our scheme with non-negligible advantage ε. Algorithm B is defined to solve the BDH problem with advantage ε'. B inputs a random instance of the BDH problem (P, aP, bP, cP) and computes $e(P,P)^{abc}$. In **Game 1**, the interaction between simulator B and adversary A is as follows:

Setup: Simulator B sets $P_{pub} = aP$ and $mpk = (P, P_{pub}, H_1, H_2)$. The response of B to the identity ID_i query is as follows:

H **-query:** Creates L and initializes it to be null. If the identity ID_i queried in (ID_i, c_i, t_i, l_i) already appears in L, it returns $H(ID_i) = h_i$, otherwise, B randomly chooses a $t_i \in Z_p^*$ and uses $Pr[c_i = 0] = \delta$ to choose $c_i \in \{0,1\}$. If $c_i = 0$, B computes $h_i = t_i bP$, otherwise, it computes $h_i = t_i P$, adds (ID_i, c_i, t_i, h_i) to L, and uses h_i response to adversary A.

H_3 **-query:** The response of simulator B to the (Y_i, ID_i) query is as follows: It creates $L_3(Y_i, ID_i, \gamma_i)$ and initializes it to null. If the (Y_i, ID_i) queried in (Y_i, ID_i, γ_i) appears in L_3, it returns $H_3(Y_i, ID_i) = \gamma_i$, adds (Y_i, ID_i, γ_i) to L_3, and uses γ_i to respond to adversary A.

Phase 1: Simulator B obtains the corresponding c_i and t_i from L. If c_i and t_i do not exist, it executes H **-query** to obtain the corresponding c_i and t_i. If $c_i = 0$, B terminates the operation, otherwise, it computes $d_{ID_i} = sH_1(ID_i) = at_i P = t_i P_{pub}$.

Challenge: Once adversary A decides that **Phase 1** is over, it outputs messages M_0 and M_1 of different lengths and broadcasts identity set $S^* = (ID_1, ID_2, \mathsf{L}, ID_n)$. Simulator B performs the following steps:

- It randomly selects $ID_0 \in S^*$, $B_i^* \in G$ and $C_0^* \in G$;

- It computes $C_1^* = r_1^* P$, $r_1^* \in Z_p$;
- It obtains the value of $H(ID_i)$ from L , and computes

$$A_i^* = k_1 + H_3\left(e\left(H_1(ID_i), P_{pub}\right)^{r_1*}, ID_i\right) \text{and } x_i^* = H(ID_i);$$

It then creates the polynomial function $f_i(x) = \sum_{j=0}^{n-1} a_{i,j} x^j$ and computes $u_i^* = \sum_{j=1}^{n} a_{j,i-1} A_j^*$, and defines challenge ciphertext $CT^* = \left(C_0^*, C_1^*, r_1^*, u_i^*, i = 0,1,\mathsf{L}\ ,n\right)$.

Phase 2: Adversary A cannot query the private key of ID_i , $ID_i \in S^*$. The response of B is the same as that of **Phase 1**.

Guess: Simulator B simulates the real attack environment of adversary A . If $c_j = 0$, $H\left(ID_j\right) = t_j bP$ and $d_{ID_j} = t_j abP$, it checks $e\left(d_{ID_j}, C_1^*\right) = e(P,P)^{t_j abr_1^*}$ and simulator randomly selects $\left(Y_j, ID_j, \gamma_j\right)$ from L_3 , parses the corresponding t_j from L and outputs $Y_j^{t_j^{-1}}$. It then defines $W_i = \left(e\left(H(ID_i), P_{pub}\right)^{r_1}, ID_i\right)$. Simulator B randomly selects $H_3(W_i)$ and $u \notin W_i$, and computes $A_i^* = u + H_3(W_i)$. In accordance with this assumption, adversary A must query H_3 on at least one W_i . We define four events as follows:

E_1 : Cannot terminate private key query;

E_2 : At least one of the identities challenging the H value contains BDH problem;

E_3 : Adversary A chooses $c_i = 0$ to distinguish the challenge information;

E_4 : Simulator B accurately selects the solution from L_3 .

Only when all events occur at the same time, can simulator B successfully solve the BDH problem. Then, it analyzes the probability of all events. The simulation B will not terminate when each $c_i = 1$ is queried based on the private key. Therefore, $Pr[Er] = Pr[c_i = 1] = (1-\delta)^{q_E}$ where $i = 1,2,\mathsf{L}\ ,q_E$.

For event 2, it computes $Pr[E_2] = \delta$. The probabilities of $c_i = 0$ and $c_i = 1$ are unknown to adversary A , because the c_i is a secret value selected by the simulator B . Therefore, $Pr[E_3] = \frac{1}{n} Pr[c_i = 0] + \frac{1}{n} Pr[c_i = 1] = \frac{1}{n}$. However, the simulator B knows that the solution to the BDH problem is in L_3 , therefore can obtain the probability $Pr[E_4] \geq \left(q_{H_3}\right)^{-1}$. We can obtain $\varepsilon' \geq Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] \cdot \varepsilon \geq (1-\delta)^{q_E} \cdot \delta \cdot \varepsilon \cdot \left(n \cdot q_{H_3}\right)^{-1}$. The function $(1-\delta)^{q_E} \cdot \delta$ is largest at $\delta_{opt} = (q_E + 1)^{-1}$. $\varepsilon' \geq \varepsilon \cdot \left(e \cdot n \cdot q_E \cdot q_{H_3}\right)^{-1}$ is based on δ_{opt} .

Theorem 2. Three hash functions H , H_2 and H_3 are defined. If an adversary of ANON-ID-CPA attacks our scheme with advantage ε , simulator B solves the BDH problem with the advantage of $\varepsilon' \geq \varepsilon \cdot \left(e \cdot n \cdot \left(q_E \cdot q_{H_2} + q_E \cdot q_{H_3}\right)\right)^{-1}$.

Proof. Compute $e(P,P)^{abc}$ in **Game 2**. H **-query**, H_3 **-query**, and **Phase 1** are the same as **Theorem 1**.

Setup: Simulator B creates $mpk=\left(P,P_{pub},H_1\right)$.

H_2**-query:** B 's response to the query of $\left(X_i,ID_i\right)$ is as follows:

$L_2\left(X_i,ID_i,\lambda_i\right)$ is initialized to be null. Simulator B checks L_2. If $\left(X_i,ID_i\right)\in L_2$, it returns $H_2\left(X_i,ID_i\right)=\lambda_i$. If not, B picks a $\lambda_i\in G$ and sets $H_2\left(X_i,ID_i\right)=\lambda_i$. Then, it adds $\left(X_i,ID_i,\lambda_i\right)$ to L_1 and responds with λ_i.

Challenge: Adversary A outputs M^*, broadcasts identity sets $S_0=\left(ID_{0,1},ID_{0,2},\text{L},ID_{0,n}\right)$ and $S_1=\left(ID_{1,1},ID_{1,2},\text{L},ID_{1,n}\right)$ without issuing private key queries to any $ID_i\in S_0\text{V}S_1$ in **Phase 1**. Simulator B executes the following steps:

- It computes $C_0^*=k_1^*+M^*$ and $C_1^*=r_1^*P$, $B_0^*\in G$, $r_1^*\in Z_p$, $k_1^*\in G$, and $ID_i\in S_0\text{V}S_1$;
- If ID_i does not exist in L, it executes H oracle, B obtains the values of $H\left(ID_i\right)$ from L, computes $x_i^*=H\left(ID_i\right)$ and creates the polynomial function $f_i\left(x\right)=\sum_{j=0}^{n}a_{i,j}x^j$;
- It randomly selects $A_i^*\in G$ for each $ID_i\in S_b\setminus S_{1-b}$. Simulator B obtains c_i and t_i from L for each $ID_i\in S_0\text{I}\ S_1$. If $c_i=0$, it computes $X_i=e\left(aP,cP\right)^{r_1^*t_i}$. If $c_i=1$ and $\left(X_i,ID_i\right)\in L_2$, it obtains λ_i and sets it as $A_i^*=\lambda_i$, otherwise, it randomly selects $A_i^*\in G$ and adds a new tuple $\left(X_i,ID_i,A_i^*\right)$ to L_2;
- It computes $Y_i=e\left(aP,cP\right)^{t_i}$. If $\left(Y_i,ID_i\right)\in L_3$, it obtains the γ_i and sets $\omega_i^*=\gamma_i$, otherwise, it picks $\omega_i^*\in G$ and adds a new $\left(Y_i,ID_i,\omega_i^*\right)$ to L_3 and compute $A_i^*=k_1^*+\omega_i^*$;
- It then computes $u_i^*=\sum_{j=1}^{n}a_{j,i-1}A_j^*$, and the ciphertext after revocation is defined as $CT^*=\left(C_0^*,C_1^*,r_1^*,u_i^*,i=\left[0,n\right]\right)$ for $i=\left[0,n\right]$.

Phase 2: Adversary A issues private key queries but cannot issue the private key on $ID_i\in S_0\text{V}S_1$.

Guess: Simulator B ignores the adversary's guess and randomly selects $\left(X_i,ID_i,\lambda_i\right)$ from L_2 or randomly chooses $\left(Y_i,ID_i,\gamma_i\right)$ from L_3. If adversary A chooses L_2, it outputs $X_j^{\left(r_2^*t_j\right)^{-1}}$ as the solution to the BDH instance, but it outputs $Y_j^{t_j^{-1}}$, if it selects L_3 as analyzed by **Theorem 1**, exiting $\varepsilon\cdot\left(e\cdot n\cdot q_E\cdot\left(q_{H_2}+q_{H_3}\right)\right)^{-1}$.

Theorem 3. Defines functions H and H_2. If there is an IND-rID-CPA adversary A that can attack our scheme with advantage ε, the algorithm B solves the BDH problem with the advantage of $\varepsilon'\geq\varepsilon\cdot\left(e\cdot n\cdot q_E\cdot q_{H_2}\right)^{-1}$.

Proof. We compute $e\left(P,P\right)^{abc}$ in **Game 3**. H **-query** and **Phase 1** are the same as **in Theorem 1**, and H_2 **-query** is the same as in **Theorem 2**.

Setup: Simulator B defines $mpk=\left(P,P_{pub},H_1,H_3\right)$.

Challenge: If adversary A did not initiate private key query to any $ID_i \in S^* \setminus R^*$, it outputs $S^* = (ID_1, ID_2, \ldots, ID_n)$, non-null revocation set $R^* = (ID_{l_1}, ID_{l_2}, \ldots, ID_{l_t})$ and two messages M_0 and M_1 of different lengths. Simulator B performs the following operations:

- It computes $C_0'^* = C_0^* + k_2^* = k_1^* + M_b + k_2^*$, $C_1^* = r_1^* P$, $ID_0 \notin S^* \cup R^*$, $A_0^*, k_1^*, k_2^* \in G$ and $r_1^* \in Z_p$;
- It parses (c_i, t_i, h_i) from L for $ID_i \in S^* \cap R^*$. If $c_i = 0$, algorithm terminates, otherwise, it computes $X_i = e(aP, cP)^{t_i}$. If $(X_i, ID_i) \in L_2$, it returns λ_i, otherwise, it randomly selects $\lambda_i \in G$. It defines $A_i^* = \lambda_i$ and a new tuple (X_i, ID_i, λ_i) is added to L_2. $ID_i \in S^* \setminus R^*$ will exist for every i. It then randomly selects $A_i^* \in G$;
- It computes $x_i^* = H_1(ID_i)$, $f_i(x) = \sum_{j=0}^{n} a_{i,j} x^j$, $A_i^* = k_1^* + H_3\left(e\left(H_1(ID_i), P_{pub}\right)^{r_1^*}, ID_i\right)$ and $u_i^* = \sum_{j=1}^{n} a_{j,i-1} A_j^*$. If there is $ID_i \in R^*$ for each i, it computes $x_i^* = H_1(ID_i)$ and creates the polynomial function $g(x) = \prod_{i=1}^{t}(x - x_i^*) = \sum_{i=1}^{t} b_i x^{i-1} \bmod p$;
- It computes $T_i^* = g(x_i)^{-1} b_i k_2^*$ for $i = 0, 1, 2, \ldots, t$. It then defines the ciphertext after revocation as $CT'^* = \left(R, C_0'^*, C_1^*, \left[u_i^*, T_i^*\right]_{i=1}^{n}\right)$.

Phase 2: Adversary A cannot query the private key on $ID_i \in S^* \setminus R^*$.

Guess: Simulator B neglects the adversary's guess and randomly selects (X_j, ID_j, λ_j) from list L_2, obtains t_j from L, and outputs $X_j^{t_j^{-1}}$. Adversary A cannot distinguish between information in security reduction. Therefore, once A outputs a terminator with a probability greater than $\frac{1}{2}$, and suppose we only consider the case that A chooses ID_i ($H(ID_i) = t_i bP$). Just like **Theorem 1**, it exists in $\varepsilon' \geq \varepsilon \cdot \left(e \cdot n \cdot q_E \cdot q_{H_2}\right)^{-1}$.

Theorem 4. Defines two functions H and H_1. If selective ANON-rID-CPA adversary A can attack our scheme with advantage ε, B can solve the BDH problem with the advantage of $\varepsilon' \geq \varepsilon \cdot \left(t \cdot q_{H_1}\right)^{-1}$. t is the number of revoked identities.

Proof. We compute $e(P,P)^{abc}$ in **Game 4**. The interactive working process between simulator B and adversary A is as follows:

Init: A generates revoke sets $R_0 = (ID_{0,1}, ID_{0,2}, \ldots, ID_{0,t})$ and $R_1 = (ID_{1,1}, ID_{1,2}, \ldots, ID_{1,t})$.

Setup: B defines $mpk = (P, P_{pub}, H_2, H_3)$, randomly selects $b \in \{0,1\}$ and $ID^* \in R_b \setminus R_{1-b}$.

H **-query:** Adversary A issues H **-query**. Simulator B responds to ID_i query as follows and creates $L(ID_i, k_i, h_i)$, which is initialized to be null:

If $ID_i \in L(ID_i, k_i, h_i)$, A returns $H(ID_i) = h_i$, otherwise, it randomly selects $k_i \in Z_p$. Simulator B sets $h_i = k_i bP$ when $ID_i = ID^*$.

H_1-query: Adversary A issues **H_1-query**. Simulator B responds to the query of (T_i, ID_i) as follows and creates $L_1(T_i, ID_i, \eta_i)$ and the list is initialized to be null:

If $(T_i, ID_i) \in L_1$, B returns $H_1(T_i, ID_i) = \eta_i$, otherwise, it selects $H_1(T_i, ID_i) = \eta_i$, $\eta_i \in G_1$ and adds (T_i, ID_i, η_i) to list L_1 .

Phase 1: Adversary A issues a private key query to $ID_i \notin R_0 \vee R_1$. The simulator obtains k_i from L and computes $d_{ID_i} = sH_1(ID_i) = ak_iP = k_iP_{pub}$.

Challenge: Adversary A outputs M^* and $S^* = (ID_1, ID_2, \ldots, ID_n)$. Simulator B executes the following steps:

- It selects $ID_0 \notin S^* \cup R_0 \cup R_1$, $k_1^* \in G$, $k_2^* \in G$, computes $C_0^* = k_1^* + k_2^* + M_b$ and $C_1^* = c^*P$;
- If there is $ID_i = ID^*$ for each $ID_i \in S^*$ and ID_0, it picks $x^* \in Z_p$, sets $x_i^* = x^*$, obtains (k_i, h_i) from L, and computes $T_i = e(aP, cP)^{k_i}$. If $(T_i, ID_i) \in L_1$, it returns η_i, otherwise, it randomly selects η_i, sets $x_i^* = \eta_i$, and adds to L_1;
- It computes $f_i(x) = \sum_{j=0}^{n} a_{i,j} x^j$ and $A_i^* = k_1^* + H_3\left(e\left(H_1(ID_i), P_{pub}\right)^{r_1^*}, ID_i\right)$, where $i = 0, 1, \ldots n$, and also computes $u_i^* = \sum_{j=1}^{n} a_{j,i-1} A_j^*$;
- For every i there is $ID_i \in R_0 \cap R_1$. It obtains (k_i, h_i) from L, and computes $T_i = e(aP, cP)^{k_i}$. It then sets $x_i^* = \eta_i$ and adds (T_i, ID_i, η_i) to L_1. It randomly selects $x_i^* \in Z_p$ for $ID^* \in R_b \setminus R_{1-b}$, and computes $g(x) = \prod_{i=1}^{t}\left(x - x_i^*\right) = \sum_{i=1}^{t} b_i x^{i-1} \bmod p$;
- It computes $T_i^* = g(x_i)^{-1} b_i k_2^*$ for any $i = 0, 1, 2, \ldots, t$ and defines the ciphertext revocation $CT'^* = \left(R, C_0'^*, C_1^*, \left[u_i^*, T_i^*\right]_{i=1}^{n}\right)$.

Phase 2: Adversary A issues a private key query on $ID_i \notin R_0 \vee R_1$. The responses of the simulator are the same as that of **Phase 1**.

Guess: If adversary A chooses ID^* to distinguish revocation set, B can successfully solve the BDH problem by computing $T^{*\frac{1}{k^*}}$. It is not difficult to compute within the scope of **Theorem 4**. Finally, the probability of choosing ID^* to break the proposed scheme is $(t-k)^{-1} \geq t^{-1} (k = |R_0 \cap R_1|)$ and we have $\varepsilon' \geq \varepsilon \cdot \left(tq_{H_1}\right)^{-1}$.

6. Performance evaluation

6.1 Comparison of functions

We analyzed the functional differences between our scheme and the other six broadcast encryption schemes. From **Table 2**, the schemes in [10,12,15] are consistent with the schemes in this paper, all of which are identity-based broadcast encryption. Combined with the changes in user privileges in smart cities, the user revocation property is used to adjust authorization

identities dynamically. The schemes in [14,15,16] achieve the user revocation property. The schemes in [10,11,16] achieve receiver anonymity. The proposed scheme has certain advantages in functions when compared with the broadcast encryption schemes in **Table 2**.

Table 2. Functional comparison

Properties	ID-based	Broadcast encryption	Revocation	Privacy-preserving
Ref [10] scheme	√	√	×	√
Ref [11] scheme	×	√	×	√
Ref [12] scheme	√	√	×	×
Ref [14] scheme	×	√	√	×
Ref [15] scheme	√	√	√	×
Ref [16] scheme	×	√	√	√
Our scheme	√	√	√	√

6.2 Theoretical analysis

The computation overhead of our scheme is compared with those of schemes [17], [18] and [19], as shown in **Table 3**. The comparison between our scheme and other schemes in terms of storage costs is shown in **Table 4**.

1) Computation overhead comparison

In **Table 3**, T_p indicates the time of bilinear pairing operation, T_e indicates the time of exponential operation, T_m indicates the time of multiplication operation, T_h indicates the time of hash operation, and T_{Inv} indicates the time of multiplication inverse operation. The operation time sequence of standard cryptographic algorithms is $T_p > T_e > T_m > T_h > T_{Inv}$, and the pairing operation T_p is longer than that of other cryptographic operations. n indicates the number of user identities in the system. From **Table 3**, the computation overheads of the four schemes grow with the increase in the number of user identities, but our scheme is the most efficient, with computation overheads $2T_h + T_p + (n+1)T_m + T_e$, $T_m + T_{Inv}$ and $T_h + T_p$, respectively.

Table 3. Computation overhead comparison

Reference	Data encrypt	ID-revoke	Data decrypt
Our scheme	$2T_h + T_p + (n+1)T_m + T_e$	$T_m + T_{Inv}$	$T_h + T_p$
Ref [17] scheme	$3T_h + 2T_p + 2(n+1)T_m + 2T_e$	$T_h + T_m$	$2T_h + 2T_p$
Ref [18] scheme	$6T_h + 2T_p + (2+n)T_m + 3T_e$	$2T_h + T_p + T_m + T_e$	$3T_h + 3T_p + T_{Inv}$
Ref [19] scheme	$2T_h + T_p + (n+2)T_m + (n+2)T_e$	$(3n+1)T_m + (2n+1)T_e$	$T_h + T_p + nT_m + nT_e$

2) Storage overhead comparison

In **Table 4**, we use $|G_1|$, $|G_T|$ and $|Z_p|$ to represent the lengths of elements in G_1, G_T and Z_p respectively. In terms of storage overhead, our scheme ($|G_1| + |G_T| + |Z_p|$) is the smallest compared with the three functions of our scheme and those of other schemes in **Table 4**. In the **Encrypt** phase, the storage overhead of the scheme in [18] is greater than that of our scheme. The storage overheads of the two other schemes are mostly the same but still larger than that of our scheme.

Table 4. Storage overhead comparison

Reference	Data encrypt	ID-revoke	Data decrypt
Our scheme	$(2+n)\|G_1\|+\|G_T\|+\|Z_p\|$	$\|G_1\|+\|Z_p\|$	$\|G_1\|+\|G_T\|+\|Z_p\|$
Ref [17] scheme	$2(2+n)\|G_1\|+\|G_T\|+\|Z_p\|$	$2\|G_1\|+(t+2)\|Z_p\|$	$(2n+2)\|G_1\|+2\|G_T\|+\|Z_p\|$
Ref [18] scheme	$10(n+1)\|G_1\|+3\|G_T\|+\|Z_p\|$	$\|G_1\|+\|G_T\|+\|Z_p\|$	$4\|G_1\|+3\|G_T\|+\|Z_p\|$
Ref [19] scheme	$2(2+n)\|G_1\|+\|G_T\|+\|Z_p\|$	$(2n+1)\|G_1\|+n\|Z_p\|$	$(n+1)\|G_1\|+\|G_T\|+\|Z_p\|$

6.3 Numerical experiment

The accuracy and efficiency of the runtime depends on the CPU. We implemented the numerical simulation experiment using a pair-based cryptographic library under the Linux operating system. Programming was based on the C language, running on a 2.60 GHz CPU and an 8 GB RAM PC.

We analyzed the computation cost of the schemes in [17], [18], [19] and the proposed scheme in terms of **Encrypt**, **Revoke**, and **Decrypt** algorithms. The users' access privileges of the other three schemes and our scheme will change. Therefore, we set the number of user identities as a variable which takes 10, 20, 30, 40, 50, and 60. In this paper, we used an average of 60 running results as the experimental results. The experimental results are shown in **Fig. 5**.

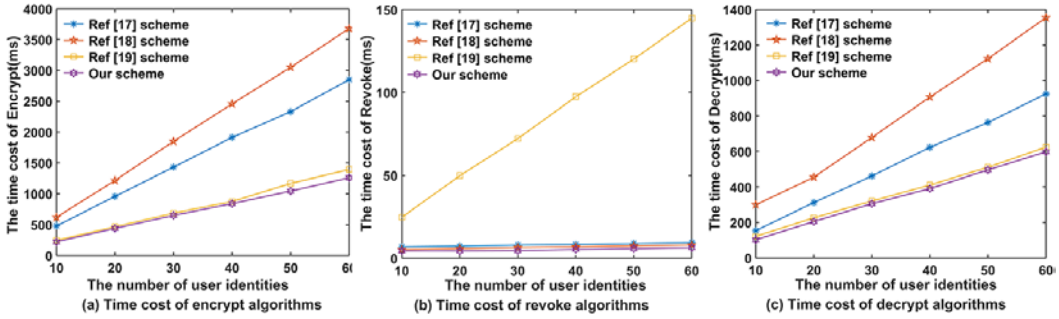


Fig. 5. (a). Comparisons of time in **Encrypt** phase; **(b).** Comparisons of time in **Revoke** phase; **(c).** Comparisons of time in **Decrypt** phase.

When there are n identities for a single identity requesting a service from the smart grid, in the Encrypt phase, the total computation overhead is $2T_h+T_p+(n+1)T_m+T_e$. It can be seen from **Fig. 5(a)** that our scheme is more efficient than other schemes and has practical application significance.

In **Fig. 5(b)**, the computation costs increase with the number of user identities, and the scheme's growth [19] is particularly notable. When the number of user identities is 60, the running time of the scheme in [19] reaches 129.5ms. As shown in **Fig. 5(b)**, the computation time of the proposed scheme is less than that of the other schemes.

As shown in **Fig. 5(c)**, we compare the computation costs of the decryption algorithm. Obviously, the decryption time of the other schemes increases with the number of users' identities. However, the time of our scheme is still a relatively small value because we only used some lightweight operations in this algorithm. In conclusion, our scheme has relative advantages compared with each phase of other schemes.

7. Conclusion

In this paper, we studied a fully privacy-preserving broadcast communication scheme and introduced how to apply cloud-network integration to the privacy-sensitive smart grid. Our proposed broadcast encryption scheme combines direct revocation and Lagrange interpolation technology. The scheme can dynamically adjust the receiver set and achieve identity anonymity. Compared with the existing schemes in terms of performance evaluation, security and other functionalities in detail, our scheme has made significant progress in performance. In future work, the proposed scheme will be used in biometric-based broadcast proxy re-encryption scenarios to obtain practical significance.

8. Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grants No. 61662071, No. 61662069, No. 61772022).

References

[1] Clohessy T, Acton T, Morgan L, et al, "Smart City as a Service (SCaaS): A Future Roadmap for E-Government Smart City Cloud Computing Initiatives," in *Proc. of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pp. 836-841, 2014. Article (CrossRef Link)

[2] Monzon A, "Smart cities concept and challenges: Bases for the assessment of smart city projects," in *Proc. of SMARTGREENS 2015-4th International Conference on Smart Cities and Green ICT Systems*, pp. 17-31, 2015. Article (CrossRef Link)

[3] Zhang Yuqing, Zhouwei, Peng Anni, "Survey of Internet of Things Security," *Journal of Research and Development*, vol. 54, no. 10, pp. 2130-2143, 2017. Article (CrossRef Link)

[4] Ejaz, Waleed, Naeem, Muhammad, Shahid, Adnan, et al, "Efficient Energy Management for the Internet of Things in Smart Cities," *IEEE Communications Magazine: Articles, News, and Events of Interest to Communications Engineers*, vol. 55, no. 1, pp. 84-91, 2017. Article (CrossRef Link)

[5] Maseleno A, Hashim W, Alicia Y C T, et al, "A Review on Smart Grid Internet of Things," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no.6, pp. 2770-2775, 2020. Article (CrossRef Link)

[6] B. C. Choi, S. H. Lee, J. C. Na, and J. H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Transactions on Consumer Electronics*, vol. 62, no.1, pp. 39-44, Feb 2016. Article (CrossRef Link)

[7] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1933-1954, Nov 2014. Article (CrossRef Link)

[8] Saleem Y, Crespi N, Rehmani M H, et al, "Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *IEEE Access*, vol. 7, pp. 62962-63003, 2019. Article (CrossRef Link)

[9] Fiat A, Naor M, "Broadcast encryption," in *Proc. of International cryptology conference*, pp. 480-491, 1993. Article (CrossRef Link)

[10] Zhang J, Mao J, "Anonymous multi-receiver broadcast encryption scheme with strong security," *International Journal of Embedded Systems*, vol. 9, no. 2, pp. 177-187, 2017. Article (CrossRef Link)

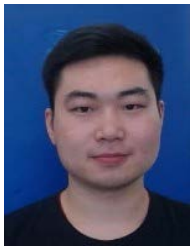
[11] Cui Yilei, Zhang Leyou, "Privacy preserving ciphertext-policy attribute-based broadcast encryption in smart city," *The Journal of China Universities of Posts and Telecommunications*, vol. 26, no. 1, pp. 21-31, 2019. Article (CrossRef Link)

[12] Li, Jiguo, Yu, Qihong, Zhang, Yichen, "Identity-based broadcast encryption with continuous leakage resilience," *Information Sciences: An International Journal*, vol. 429, pp. 177-193, 2018. Article (CrossRef Link)
[13] JIA Hongyong, CHEN Yue, YANG Kuiwu, et al, "Revocable Broadcast Encryption with Constant Ciphertext and Private Key Size," *Chinese Journal of Electronics*, vol. 28, no. 4, pp. 690-697, 2019. Article (CrossRef Link)
[14] ZHU Yan, YU Ruyun, CHEN E, et al, "An Efficient Broadcast Encryption Supporting Designation and Revocation Mechanisms," *Chinese Journal of Electronics*, vol. 28, no. 3, pp. 445-456, 2019. Article (CrossRef Link)
[15] Dawei Li, Jianwei Liu, Zongyang Zhang, et al, "Revocable Hierarchical Identity-Based Broadcast Encryption," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 539-549, 2018. Article (CrossRef Link)
[16] Yi X, Paulet R, Bertino E, et al, "Practical Anonymous Subscription with Revocation Based on Broadcast Encryption," in *Proc. of 2020 IEEE 36th International Conference on Data Engineering (ICDE)*, pp. 241-252, 2020. Article (CrossRef Link)
[17] Lai J, Mu Y, Guo F, et al, "Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing," in *Proc. of Australasian conference on information security and privacy*, pp. 223-239, 2016. Article (CrossRef Link)
[18] Lai J, Mu Y, Guo F, et al, "Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city," *Personal and Ubiquitous computing*, vol. 21, no. 5, pp. 855-868, 2017. Article (CrossRef Link)
[19] Lai, Jianchang, Guo, Fuchun, Mu, Yi, et al, "Fully Privacy-Preserving ID-Based Broadcast Encryption with Authorization," *The Computer journal*, vol. 60, no. 12, pp. 1809-1821, 2017. Article (CrossRef Link)
[20] Wang X, Dai H, Zhang K, et al, "Secure and flexible economic data sharing protocol based on ID-based dynamic exclusive broadcast encryption in economic system," *Future Generation Computer Systems*, vol. 99, pp. 177-185, 2019. Article (CrossRef Link)
[21] Guo D, Wen Q, Jin Z, et al, "Authenticated public key broadcast encryption with short ciphertexts," *Multimedia Tools and Applications*, vol. 78, pp. 23399–23414, 2019. Article (CrossRef Link)
[22] Leyou Zhang, Qing Wu, Yi Mu, "Anonymous Identity-Based Broadcast Encryption with Adaptive Security," *Cyberspace safety and security*, pp. 258–271, 2013. Article (CrossRef Link)
[23] Waters B, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," *Public key cryptography*, vol. 6571, pp. 53–70, 2011. Article (CrossRef Link)

Shufen Niu was born in Tongwei, Gansu, China, in 1976. She received the Bachelor of Science degree from Northwest Normal University, in 2000, the Master of Science degree in operations research and cybernetics from Shanghai University, in 2007, and the Ph.D. degree in cryptography from Northwest Normal University, in 2013. From March 2018 to January 2019, she was a Visiting Scholar with the Department of Computer Science at Georgia State University. She is currently teaching at the School of Computer Science and Engineering, Northwest Normal University. She is also an Associate Professor and a Master Tutor. In recent years, she has published many excellent articles and hosted several National Natural Science Foundation projects. She presided over the Northwest Normal University Young Teacher Research Promotion Program. Her research direction is cryptography. She received the second prize for scientific and technological progress in colleges and universities in Gansu Province, in 2012, and the third prize for scientific and technological progress in colleges and universities in Gansu Province, in 2013. (Email: sfniu76@nwnu.edu.cn)

Lizhi Fang was born in Zhangye, Gansu, China, in 1993. She received her bachelor's degree from the School of Computer Science and Engineering, Northwest Normal University, in 2018. She is currently pursuing a master's degree at the School of Computer Science and Engineering, Northwest Normal University. Her research direction is cryptography. (Email: 1439902640@qq.com)

Song Mi was born in Nanyang, Henan, China, in 1996. She received her bachelor's degree from the School of Electronics and Information Engineering, Jinggangshan University, in 2018. She is currently pursuing a master's degree at the School of Computer Science and Engineering, Northwest Normal University. Her research direction is cryptography. (Email: 1744391811@qq.com)



Yu Fei was born in Jining, Shandong, China, in 1997. He received his bachelor's degree from the School of Software, Jishou University, in 2019. He is currently pursuing a master's degree at the School of Computer Science and Engineering, Northwest Normal University. His research direction is cryptography. (Email: yf_1997163@163.com)

Han Song was born in Puyang, Henan, China, in 1996. He received his bachelor's degree from the School of Software, Zhengzhou University, in 2019. He is currently pursuing a master's degree at the School of Computer Science and Engineering, Northwest Normal University. His research direction is cryptography. (Email: 565904313@qq.com)