applied sciences

MDPI

Article

Anonymous Identity Based Broadcast Encryption against Continual Side Channel Attacks in the State Partition Model

Qihong Yu [1,*], Jiguo Li [2] and Sai Ji [1]

[1] College of Information Engineering, Suqian University, Suqian 223800, China
[2] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
* Correspondence: yuqhsqu@163.com or qhyu@squ.edu.cn

Abstract: In the past 10 years, many side-channel attacks have been discovered and exploited one after another by attackers, which have greatly damaged the security of cryptographic systems. Since no existing anonymous broadcast encryption scheme can resist the side-channel attack, the paper presents an anonymous identity-based broadcast encryption against continual side-channel attacks in the state partition model (CLR-SS-AIBBE). Based on split-state technology, the proposed scheme divides the private key into two states, and the decryption operations are correspondingly divided into two steps. Based on the three static hypotheses for a bilinear group with composite order, the proposed scheme can be proved to be fully secure by the dual system encryption technology in the standard model. The leakage ratio about the private key can reach 1/3.

Keywords: side-channel attack; split-state; composite order group; broadcast encryption; anonymity

Citation: Yu, Q.; Li, J.; Ji, S. Anonymous Identity Based Broadcast Encryption against Continual Side Channel Attacks in the State Partition Model. *Appl. Sci.* **2022**, *12*, 9395. https://doi.org/10.3390/app12189395

Academic Editor: David Megías

Received: 26 August 2022
Accepted: 13 September 2022
Published: 19 September 2022

1. Introduction

In the past 10 years, cryptography has made great progress in expanding the adversary model to cover side-channel attacks [1–4], and researchers have built some provably secure cryptographic schemes that can resist some side-channel attacks. In most theoretical work, it is assumed that the participants have complete confidentiality to their local computation. The attacker may only obtain the signature of the selected plaintext or the decryption of the selected ciphertext, but it is usually assumed that the signature or encryption process itself is completely secret to the adversary. In particular, theoretically, the related information of the private key that an adversary can obtain is only contained in a clear boundary, such as signature or decryption. Such adversaries are sometimes called "black box" attackers. Goldwasser and Micali pioneered work for modern cryptography. Based on some computational complexity assumptions, they proved the security of many cryptographic schemes under the black box model, such as encryption [5], signature [6] and the zero-knowledge proof [7].

However, real attackers do not always follow such clear boundaries. Various successful side-channel attacks have proven that the key information and internal state information related to the specific calculation may be leaked to a certain adversary. Since each cryptographic algorithm is ultimately implemented on the physical platform, it will inevitably affect the surrounding environment in a measurable way. The side-channel attack obtains secret information about the cryptographic system by measuring the surrounding environment of the machine that is executing the related algorithms. For example, an attacker obtains the relevant confidential information of the cryptographic system by measuring and analyzing the time [4] or the electromagnetic radiation [8] of the specific algorithm. Through the "cold start" attack [9], if an adversary can access the corresponding physical device, it can recover part of the key of the cryptographic system even when the power has just been cut off. Side-channel attacks [10,11] allow processes to violate isolation boundaries and read information from other processes on the same machine. In other words, the real attacker may not be the black box.

The emergence of side-channel attacks leads cryptographers to reevaluate the black box model and create new adversary models and provable security schemes. This work is called leakage-resilient cryptography.

As leakage-resilient cryptography is a relatively young research direction of cryptography, the theory and practice of leakage-resilient cryptography have made remarkable achievements in the past decade.

2. Related Work and Our Motivations

2.1. Leakage-Resilient Cryptography

Leakage-resilient (LR) cryptosystems are the cryptographic systems that are secure against side-channel attacks. The attack capability depends on specific limitations, which are usually abstracted as a leak function in the security model. According to different restrictions on the leakage function, the current leakage-resilient cryptography models are mainly as follows.

(1) "Only calculation leaks"

Micali et al. [12] proposed the concept of "only calculation leaks" (OCL): it is required that the leakage can only occur in the computing portion, so the portion that does not participate in the computing does not leak information. The total leakage amount and the leakage function form are not limited. In this model, Dziembowski et al. [13] proposed a secure stream cipher scheme. Goldwasser et al. [14] constructed one time scheme, which was later widely used in other schemes.

(2) Bounded-leakage model

For a cold start attack, even parts that do not participate in the computation can leak information. To solve this problem, Akavia et al. [15] gave the concept of bounded-leakage model (BLM). It is required that the leakage function has a bounded output. Naor et al. [16] extended the concept of bounded leakage and presented the entropy-bounded-leakage model. There is no requirement on the output length about the leakage function, only that the system's secret information derived from the leakage function has a bounded entropy loss.

Akavia et al. [15] gave a specific public key encryption (PKE) scheme and an identity-based encryption scheme, which are leakage-resilient. Naor et al. [16] used the hash proof system (HPS) to obtain an encryption scheme with chosen plaintext attack (CPA) security and an encryption scheme with chosen ciphertext attack (CCA2) security, which resist side-channel attacks. The leakage rate of the private key for their scheme with CCA2 security can only reach one-sixth. Luo et al. [17] proposed a lattice-based PKE scheme. The paper [18] presented an effective LR PKE. The work [19] used anonymous HPS to construct an anonymous LR PKE. Li et al. [20] gave an efficient leakage-resilient identity-based encryption scheme.

Following the basic requirement of the "only calculation leaks" model and bounded-leakage model, Prouf et al. [21] introduced the noise-leakage model, which can capture the power consumption and electromagnetic leakage well. Duc et al. [22] proposed the random detection model, which includes noise leakage.

Unlike the construction of LR cryptosystems through specific number theory and algebraic hypothesis, Hazay et al. [23] constructed LR PKE schemes through any standard PKE under general and minimum assumptions. Only if a one-way function exists, then they can construct LR symmetric key encryption, etc.

Galindo et al. [24] weakened the limitations on the leakage function and only required that the output of the leakage function has sufficient minimum entropy. What is more, they did not limit the amount of leakage. The safety of their scheme was proven by using the general bilinear group theory. They proposed a scheme that was easily implemented by coding technology, and the scheme was implemented by software based on the MIRACL library.

Genkin et al. [25] designed hardware devices for the zero-knowledge proof and general multiparty computation. This construction can unconditionally capture the "only

calculation leaks" of the real side-channel attack. They provided different tradeoffs between efficiency and security.

(3) Continual leakage model

When the side-channel attack continues, the leakage may gradually increase and eventually exceed the given limit. BLM cannot solve this problem. Both refs. [26,27], respectively, presented the concept of the continuous-leakage model (CLM). Their main idea is to refresh the secret key periodically. The restrictions are that the leakage is bounded between two consecutive updates. The leakage of the whole process can be unlimited. The paper [28] gives a dynamic secret-sharing scheme with continual leakage resilience by using the state partition technique. The paper [29] proposed a hierarchical attribute-based encryption that resists a continuous-leakage attack.

The relationship about the three leakage models is given in Figure 1.

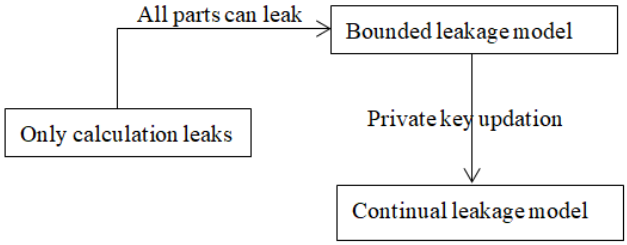

Figure 1. The relationship between the three leakage models.

The "only calculation leaks" model allows information leakage only in the part currently performing the calculation of a cryptographic system. If we consider that there may be information leakage in the part that does not participate in calculation, the bounded-leakage model can solve the problem. In order to solve the problem that the leaked information will gradually exceed the given limit, given that it is necessary to update the key periodically, the continuous-leakage model is produced.

2.2. Identity-Based Broadcast Encryption

Ref. [30] provided the broadcast encryption (BE) scheme. From then on, many BE schemes have been proposed [31–33]. Broadcast encryption is widely used to multicast communication, copyright management, et al. For example, to solve the redundancy problem in information transmission for the vehicular ad hoc network, Zhong et al. [34] used broadcast encryption as the secure data sharing scheme from vehicle to infrastructure communication mode.

Ref. [35] constructed the first identity-based BE (IBBE) under the random oracle model (ROM). Since then, scholars have conducted in-depth research on IBBE from the aspects of efficiency and special performance, obtaining many achievements. Ren et al. [36] designed an IBBE scheme and proved its security in the standard model (STDM). In their proposed scheme, the length of ciphertext and public key are fixed. Zhang et al. [37] gave an IBBE in STDM and proved its security with dual-system technology. Their scheme has a fixed private key and ciphertext length. The anonymous IBBE constructed by Libert et al. [38] has a ciphertext that is not fixed in length and is positively related to the number of recipients.

The anonymous IBBE given by Zhang et al. [39] has a fixed ciphertext length, but the key is too long. The scheme is provably safe under STDM through dual-system technology. Li et al. [40] gave an anonymous certificate-based broadcast encryption. Lai et al. [41] gave an IBBE from inner products with fixed private key length, which supported infinite private key query in ROM. Jiang et al. [42] proposed an efficient IBBE with keyword search in cloud computing. It provides data retrieval and resists internal attack. Zhao et al. [43] presented a weak black box IBBE scheme in ROM, which has fixed private key size and public traceability for ciphertext. The tracking was performed through employing a public key of some suspicious user instead of its private key. Chen et al. [44] gave an efficient

identity based anonymous broadcast encryption for cloud storage services, which has a fixed size for its public parameters, private key and ciphertext.

2.3. Our Motivations

Xiong et al. [28] presented a secret-sharing scheme that can resist side-channel attacks by the split-state technology. Since then, state partition technology has been gradually used to construct some cryptographic schemes with special performance. Liu et al. [45] ensured the security of their scheme in the case of continuous state partition leakage and tamper attacks from an algorithmic point of view by means of general reference string and nonmalleable code.

Faonio et al. [46] divided the code into two parts. By using a refresh process based on state division, non-extensible code has the ability to resist persistent leakage attacks. In these schemes based on state division technology, the state is usually divided into two parts. The state is sometimes divided into four or eight parts [47,48].

Since dual-system technology [49] was used to prove the security for cryptosystems, a lot of work has been carried out along this line. In view of bilinear groups with composite order, the orthogonality of subgroup elements can be fully utilized to carry effective information and hide invalid information. It is usually used to finish the security proof in combination with dual-system encryption technology. Refs. [50–52] achieve some schemes with leakage resilience through dual-system technology.

For the anonymous broadcast encryption, there is no leakage-resilient scheme at present. On the basis of the reference [53], we present an anonymous broadcast encryption scheme against the continuous leakage of a private key.

2.4. Our Contributions

We put forward an anonymous IBBE against a continual-leakage attack. First, for the first time, we use state division technology to obtain the leakage resilience of a broadcast encryption scheme. The main advantage is that it can ensure that the scheme has the ability to resist side-channel attacks and has relatively high computational efficiency at the same time. The computational efficiency is also one of the important considerations of the cryptographic scheme. Second, the scheme has anonymity, which protects the privacy of users. For example, for a health diagnosis and treatment system based on cloud storage, if the data owner (a hospital) wants to encrypt the data about coronary heart disease in the Department of Cardiology for the relevant patients, if there is no anonymity, a bystander can infer that a user accessing this data is suffering from heart disease. Thus, the identity information of the user is virtually leaked. Therefore, anonymity is also a very important aspect. In fact, ref. [53] provided an anonymous broadcast encryption. Although its efficiency is considered, a side-channel attack is not considered. Thirdly, our scheme has a good ability to resist a side-channel attack. The side-channel attack is a new cryptosystem attack form in the past 10 years. Therefore, if the designed cryptographic algorithm can capture the side-channel attacks, the security for the cryptographic scheme is better.

Figure 2 shows a whole framework about an anonymous leakage-resilient IBBE for cloud services. The system involves four entities: private key generator (PKG), cloud storage server (CSS), data user (DU) and data owner (DO). The PKG offers private keys for all DUs based on DUs' identities. The PKG sends the system's parameters to the DO and DU. The DO will authorize the data user in the target set as the receiver and encrypt the symmetric encryption key through anonymous IBBE. The DO encrypts its information by the session key and places the ciphertext on CSS. The symmetric encryption key is broadcast by the data owner to the target user set. The target user decrypts the ciphertext with their private key and obtains a symmetric encryption key. Next, the target user decrypts the ciphertext with the symmetric encryption key. In this process, the user cannot obtain the information of other users, so the system has anonymity.

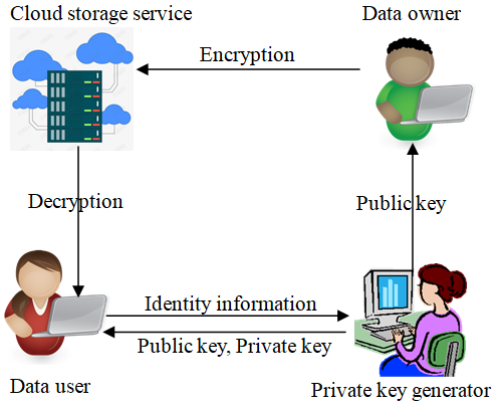

Figure 2. The system's framework of anonymous leakage-resilient IBBE in cloud storage services.

3. Related Knowledge

We give some notations in Table 1 and give the preliminaries that will be used in the paper.

Table 1. Some notations.

Notation	Description
G_1, G_2	Cyclic groups
$N = w_1w_2w_3$	Order of G_1 and G_2
Φ	Bilinear group generation algorithm
G_{w_1}, G_{w_2}, G_{w_3}	Subgroups of G_1 for order w_1, w_2 and w_3
ϖ	Safety parameter
X_1	Random value of G_{w_1}
X_2, Y_2, Z_2	Random values of G_{w_2}
X_3, Y_3	Random values of G_{w_3}
MP	Public parameters
MK	Master private key
$SK_{ID,k}$	Private key for identity ID
$SK_{ID,k+1}$	Updated private key
M	A plaintext
CT	A ciphertext
$\mathcal{A}$	An adversary
$\mathcal{B}$	A challenger
L_{SK}	Bound for private key leakage
EX_R	Real security game

3.1. Bilinear Group

Definition 1. *Suppose that G_1 and G_2 are multiplicative cyclic group with order N. Suppose that a is a generator of group G_1. A map $e : G_1 \times G_1 \to G_2$ is called as bilinear map, if it satisfies the conditions as follows.*

(1) Bilinearity: $\forall a, b \in G_1$ and for $\forall u, v \in Z^*$, it holds that $e(a^u, b^v) = e(a, b)^{uv}$.
(2) Non degeneracy: $\forall a, b \in G_1$, $e(a, b) \neq 1_{G_2}$.
(3) Computability: There is an effective algorithm to calculate $e(a, b)$.

3.2. Composite Order Bilinear Groups

Ref. [54] put forward the concept of composite order bilinear groups. Let Φ represent a bilinear group generation algorithm. Taking the safety parameters ϖ as inputs, Φ can produce a bilinear group with composite order $\Omega = \{N = w_1w_2w_3, G_1, G_2, e\}$. w_1, w_2 and w_3 are three different primes with θ bits (that is, $\log_2^{w_1} = \log_2^{w_2} = \log_2^{w_3} = \theta$). G_1 is a cyclic group with order $N = w_1w_2w_3$, so is G_2. e is a bilinear map that maps $G_1 \times G_1$ to G_2. θ is determined by safety parameter ϖ.

Let G_{w_1}, G_{w_2} and G_{w_3} denote the subgroups of order w_1, w_2 and w_3, respectively, in the group G_1. Let $G_{w_1w_2}$ denote the subgroup of order w_1w_2 in G_1. If an element Y can be written as the product of an element in G_{w_1} and an element in G_{w_2}, then these two parts are called the part G_{w_1} of Y and the part G_{w_2} of Y, respectively. Assuming that $p_i \in G_{w_i}$ and $p_j \in G_{w_j}$ $(i \neq j)$, we can acquire $e(p_i, p_j) = 1$. So, G_{w_i} and G_{w_j} are orthogonal. For example, G_{w_1} and G_{w_2} are orthogonal. Suppose g is a generator of G_1, $g^{w_1w_2}$ is a generator of G_{w_3}, $g^{w_1w_3}$ is a generator of G_{w_2}, and $g^{w_2w_3}$ is a generator of G_{w_1}. Then, there are α_1 and α_2, such that $p_1 = (g^{w_2w_3})^{\alpha_1}$ and $p_2 = (g^{w_1w_3})^{\alpha_2}$. Therefore, $e(p_1, p_2) = e(g^{w_2w_3\alpha_1}, g^{w_1w_3\alpha_2}) = e(g^{\alpha_1}, g^{w_3\alpha_2})^{w_1w_2w_3} = 1$. So, G_{w_1} and G_{w_2} are orthogonal.

Three assumptions [49,51] are given below. Suppose g_i is the generator of G_{w_i}.

Assumption 1. *Let Φ generate a bilinear group. Given the following distribution:*

$\Omega = \{N = w_1w_2w_3, G_1, G_2, e\} \xleftarrow{R} \Phi$, $g_1 \xleftarrow{R} G_{w_1}, X_3 \xleftarrow{R} G_{w_3}$, $U = (\Omega, g_1, X_3)$. *No adversary can distinguish $T_1 \in G_{w_1w_2}$ from $T_2 \in G_{w_1}$.*

The superiority that one adversary destroys Assumption 1 is denoted by $Adv_{\psi,\mathcal{A}}(\varpi) = \left|\mathrm{Su}[\mathcal{A}(U, T_1) = 1] - \mathrm{Su}[\mathcal{A}(U, T_2) = 1]\right|$.

If $Adv_{\psi,\mathcal{A}}(\varpi)$ can be ignored, Assumption 1 is considered valid.

Assumption 2. *Let Φ generate a bilinear group. Given the following distribution:*

$\Omega = \{N = w_1w_2w_3, G_1, G_2, e\} \xleftarrow{R} \Phi, X_1, g_1 \xleftarrow{R} G_{w_1}, X_2, Y_2 \xleftarrow{R} G_{w_2}, X_3, Y_3 \xleftarrow{R} G_{w_3}$, $U = (\Omega, g_1, X_1X_2, X_3, Y_2Y_3)$. *No adversary can distinguish $T_1 \in G$ from $T_2 \in G_{w_1w_3}$.*

The superiority that one adversary destroys Assumption 2 is denoted by $Adv_{\psi,\mathcal{A}}(\varpi) = \left|\mathrm{Su}[\mathcal{A}(U, T_1) = 1] - \mathrm{Su}[\mathcal{A}(U, T_2) = 1]\right|$.

If $Adv_{\psi,\mathcal{A}}(\varpi)$ can be ignored, Assumption 2 is considered valid.

Assumption 3. *Let Φ generate a bilinear group. Given the following distribution:*

$\Omega = \{N = w_1w_2w_3, G_1, G_2, e\} \xleftarrow{R} \Phi$, $\alpha, s \xleftarrow{R} Z_N$, $g_1 \xleftarrow{R} G_{w_1}, X_2, Y_2, Z_2 \xleftarrow{R} G_{w_2}$, $X_3 \xleftarrow{R} G_{w_3}$, $U = (\Omega, g_1, g_1^{\alpha}X_2, X_3, g_1^{s}Y_2, Z_2)$. *No adversary can distinguish $T_1 \xleftarrow{R} e(g_1, g_1)^{\alpha s}$ from $T_2 \xleftarrow{R} G'$.*

The superiority that one adversary destroys Assumption 3 is denoted by $Adv_{\psi,\mathcal{A}}(\varpi) = \left|\mathrm{Su}[\mathcal{A}(U, T_1) = 1] - \mathrm{Su}[\mathcal{A}(U, T_2) = 1]\right|$.

If $Adv_{\psi,\mathcal{A}}(\varpi)$ can be ignored, Assumption 3 is considered valid.

4. Syntax and Security Description of CLR-SS-AIBBE

4.1. Syntax of CLR-SS-AIBBE

Inspired by refs. [50,51,53], a formal definition of CLR-SS-AIBBE is given.

Initialization algorithm: Start$(\varpi, l) \rightarrow (MP, MK)$. The algorithm inputs the maximum value l of users and security index ϖ as inputs. It generates the public parameter (or master public key), MP, and the master private key, MK. MP is open to all users. MK is kept as a secret.

Private key generation algorithm: KeyGen$(MP, MK, ID) \rightarrow SK_{ID}$. The algorithm inputs MP, MK and one user's identity ID. It obtains the user's private key $SK_{ID} = (SK_{ID,0,1}, SK_{ID,0,2})$.

Private key updation algorithm: KeyUpd$(MP, SK_{ID,k}) \rightarrow SK_{ID,k+1}$. It inputs $SK_{ID,k}$ and MP. It obtains a new private key $SK_{ID,k+1}$.

Encryption algorithm: Encrypt$(MP, M, S) \rightarrow CT$. The algorithm inputs MP, the message M and an identity set $S = \{ID_1, \ldots, ID_d\}$ $(d \leq l)$ and obtains (Hdr, CK), where CK is a symmetric key, and Hdr is called the header. When the broadcaster is going to send the ciphertext of the message, M, to the users in S, the broadcaster obtains C by encrypting the M by CK, which generates the ciphertext $CT = (C, Hdr)$ and broadcasts (C, Hdr, S).

Decryption algorithm 1: Decrypt1$(MP, SK_{ID_i,k,1}, S, CT) \rightarrow CT'$. The algorithm inputs the master public key MP, private key $SK_{ID_i,k,1}$, users' identity set S and ciphertext

CT. First, it divides CT into (C, Hdr). If $ID_i \in S$, the algorithm uses Hdr to produce some part related to the plaintext.

Decryption algorithm 2: Decrypt$2(MP, SK_{ID_i,k,2}, S, CT') \rightarrow M$. The algorithm inputs the master public key MP, private key $SK_{ID_i,k,2}$, users' identity set S and ciphertext CT'. If $ID_i \in S$, it first calculates the CK. Then, the plaintext message is recovered by decrypting C.

Semi-functional private key generation algorithm: KeyGenSF$(MP, MK, ID) \rightarrow \widetilde{SK_{ID}}$. It inputs MP, MK and an identity ID. It outputs the semi-functional private key $\widetilde{SK_{ID}}$.

Semi-functional encryption algorithm: EncryptSF$(MP, M, S) \rightarrow \widetilde{CT}$. The algorithm inputs MP, S and M. Semi-functional ciphertext $\widetilde{CT}$ is generated.

The first three algorithms are run by the private key generation center, and other algorithms are run by the user. The last two algorithms are only used for the security proof. Both decryption algorithm 1 and decryption algorithm 2 are executed by the data user. They are usually executed on two components and then transmit information through a secure channel. Each component operates independently and suffers from side-channel attacks. In this way, security can be enhanced.

4.2. Security Description of CLR-SS-AIBBE

Our scheme is secure against the chosen ciphertext attack.

The security of the **CLR-SS-AIBBE** scheme is described by the upcoming game EX_R. In EX_R, the challenger $\mathcal{B}$ holds a list $\mathcal{L} = \{(\mathcal{H}, \mathcal{I}, \mathcal{SK}, \mathcal{LK}_1, \mathcal{LK}_2)\}$, where $\mathcal{H}$, $\mathcal{I}$, $\mathcal{SK}$ and $\mathcal{LK}_1, \mathcal{LK}_2$ are the handle's space, the identity's space, the private key's space and the leakage space, respectively. Let $\mathcal{H} = \mathbb{N}$ and $\mathcal{LK}_1 = \mathcal{LK}_2 = \mathbb{N}$.

The game EX_R is played by an adversary (or attacker), $\mathcal{A}$, and a challenger, $\mathcal{B}$.

EX_R:

Initialization: $\mathcal{B}$ calls the initialization algorithm to gain MP and MK. $\mathcal{B}$ sends MP to $\mathcal{A}$.

Stage 1. *An attacker can query these upcoming oracles.*

$\mathcal{O}$-*Generate*(ID). As for one identity ID, $\mathcal{B}$ finds its corresponding item in $\mathcal{L}$. If one item is found out, the game is over. If no item is found out, $\mathcal{B}$ runs **KeyGen** to obtain one private key SK_{ID} and updates the handle $h \leftarrow h + 1$. Then, the challenger puts $(h, ID, SK_{ID}, 0, 0)$ in $\mathcal{L}$.

$\mathcal{O}$-*Leak*(h, f_1, f_2). The attacker inquires the leakage of the private key about the item h. The attacker selects two leakage functions, f_1 and f_2. f_1 and f_2 input the private keys $SK_{ID_i,k,1}$ and $SK_{ID_i,k,2}$, respectively. $\mathcal{B}$ sends the outputs of f_1 and f_2 to the adversary.

Specifically, $\mathcal{B}$ looks for one corresponding item about the handle h. If one item $(h, ID, SK_{ID}, L_1, L_2)$ is found out, $\mathcal{B}$ determines whether $L_1 + \left|f_1(SK_{ID})\right| \leq L_{SK_1}$ and $L_2 + \left|f_2(SK_{ID})\right| \leq L_{SK_2}$, where L_{SK_1} and L_{SK_2} are the maximum values that allow the leakage of the private key. If $L_1 + \left|f_1(SK_{ID})\right| \leq L_{SK_1}$, the challenger will send $f_1(SK_{ID})$ to the adversary and use $(h, ID, SK_{ID}, L_1 + |f_1(SK_{ID})|, L_2)$ to update $(h, ID, SK_{ID}, L_1, L_2)$. Otherwise, the challenger outputs $\perp$. Similarly, if $L_2 + \left|f_2(SK_{ID})\right| \leq L_{SK_2}$, the challenger will send $f_2(SK_{ID})$ to the adversary and use $(h, ID, SK_{ID}, L_1, L_2 + |f_2(SK_{ID})|)$ to update $(h, ID, SK_{ID}, L_1, L_2)$. Otherwise, the challenger outputs $\perp$. Set $L_{SK_1} = L_{SK_2} = L_{SK}$.

$\mathcal{O}$-*Reveal*(h). If $\mathcal{A}$ asks for a private key about one handle h, $\mathcal{B}$ looks for it in $\mathcal{L}$. If the found item is $(h, ID, SK_{ID}, L_1, L_2)$, the challenger sends SK_{ID} to $\mathcal{A}$.

$\mathcal{O}$-*Refersh*. If an attacker enquires an updated private key about the handle h, the challenger looks for it in $\mathcal{L}$. If the found item is $(h, ID, SK_{ID}, L_1, L_2)$, the challenger invokes **KeyUpd** to obtain the updated private key $\widehat{SK_{ID}}$. $\mathcal{B}$ sends $\widehat{SK_{ID}}$ to $\mathcal{A}$ and uses $(h, ID, \widehat{SK_{ID}}, 0, 0)$ to update $(h, ID, SK_{ID}, L_1, L_2)$.

$\mathcal{O}$-*Decrypt*1. If the attacker asks for the corresponding plaintext of (ID, CT), the challenger looks for SK_{ID} in $\mathcal{L}$. The challenger runs **Decrypt**$1(MP, SK_{ID_i,k,1}, S, CT) \rightarrow CT'$. If $ID_i \in S$, the challenger calculates some parts CT' of the plaintext and sends CT' to $\mathcal{A}$.

$\mathcal{O}$-*Decrypt*2. If $\mathcal{A}$ inquires about this plaintext of (ID, CT), the challenger looks for SK_{ID} about ID in $\mathcal{L}$. This challenger runs **Decrypt**2$(MP, SK_{ID_i,k,2}, S, CT') \rightarrow M$. First, CT is divided into (C, Hdr). If $ID_i \in S$, the challenger uses Hdr to calculate the symmetric key CK. Then, it recovers M by decrypting C with CK and sends it to $\mathcal{A}$.

Challenge. $\mathcal{A}$ gives two messages, M_0 and M_1, of equal size. $\mathcal{B}$ selects randomly $\beta \leftarrow \{0,1\}$. Then, $\mathcal{B}$ takes MP and the identity set $S^* = \{ID_1^*, \ldots, ID_d^*\}$ $(d \leq l)$ as input. $\mathcal{B}$ outputs (Hdr^*, CK^*). $\mathcal{B}$ utilizes CK^* to encrypt M_β to get the ciphertext C^*. $\mathcal{B}$ sends (C^*, Hdr^*, S^*).

Stage 2. *$\mathcal{A}$ can ask $\mathcal{O}$-Create, $\mathcal{O}$-Reveal, $\mathcal{O}$-Decrypt*1 *and $\mathcal{O}$-Decrypt*2*. The basic limitations are the same as stage 1. Other restrictions are that $\mathcal{A}$ cannot inquiry the information about $ID \in S^*$ and $Hdr = Hdr^*$. In addition, a leakage inquiry cannot be performed. Since, if a leakage inquiry is allowed, $\mathcal{A}$ may take the ciphertext, the decryption algorithm and M_0 and M_1 as the input of the leakage function and obtain a bit output, and win the game in an ordinary way.*

Guess. The attacker gives one guess, $\beta' \in \{0,1\}$. If $\beta' = \beta$, $\mathcal{A}$ wins this game $\mathrm{EX_R}$. The superiority, that $\mathcal{A}$ wins this game $\mathrm{EX_R}$, is defined as $Adv_{\mathcal{A}}(L_{SK}) = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right|$.

If any PPT attacker can only win negligible advantages in the game $\mathrm{EX_R}$, the CLR-SS-AIBBE scheme is said to be safety against leakage attack.

5. Specific Construction of CLR-SS-AIBBE

Let Φ to represent a bilinear group generation algorithm. Taking the safety parameters ϖ as inputs, Φ produces a bilinear group with composite order $\Omega = \{N = w_1 w_2 w_3, G_1, G_2, e\}$. w_1, w_2 and w_3 are three different primes with θ bits (that is, $\log_2^{w_1} = \log_2^{w_2} = \log_2^{w_3} = \theta$). G_1 is a cyclic group with order $N = w_1 w_2 w_3$, so is G_2. e is a bilinear map that maps $G_1 \times G_1$ to G_2. θ is determined by safety parameter ϖ.

Initialization algorithm. Let l indicate the maximum number of users. The algorithm randomly selects $g_1, h_1 \in G_{w_1}, g_3 \in G_{w_3}$, $a_1, a_2, \ldots, a_l, b \in Z_N$ and $\alpha \in Z_N$ and sets $u_1 = g_1^{a_1}, \ldots, u_l = g_1^{a_l}$ and $h_1 = g_1^b$. The master public key is $MP = \{N, g_1, g_3, h_1, u_1, \ldots, u_l, e(g_1, g_1)^\alpha\}$. The master private key is $MK = \{\alpha\}$.

Private key generation algorithm. For an identity $ID_i \in S$, where $S = (ID_1, \ldots, ID_d)$ $(d \leq l)$ is this set of the intended recipients, the algorithm inputs MP, MK and one user's identity, ID_i. The algorithm randomly selects $a_1, a_2, \ldots, a_d, b \in Z_N$, $\beta_{i,0}, \gamma_{i,0} \in Z_N$, $r_i \in Z_N (i = \{1, \ldots, d\})$ and $R_i, Q_i, R_i', Q_i' \in G_{p_3}$. It sets $u_1 = g_1^{a_1}, \ldots, u_l = g_1^{a_l}$ and $h_1 = g_1^b$. The generated private key is $SK_{ID_i,0} = (SK_{ID_i,0,1}, SK_{ID_i,0,2})$, where $SK_{ID_i,0,1} = (g_1^{r_i} R_i g_1^{\beta_{i,0}}, g_1^\alpha (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_i g_1^{\gamma_{i,0}})$ and $SK_{ID_i,0,2} = (R_i' g_1^{-\beta_{i,0}}, Q_i' g_1^{-\gamma_{i,0}})$.

Private key update algorithm. It inputs $SK_{ID_i,k}$ and MP. It obtains a new private key $SK_{ID_i,k+1}$. For the private key $SK_{ID_i,k} = (SK_{ID_i,k,1}, SK_{ID_i,k,2})$, where $SK_{ID_i,k,1} = (SK^1_{ID_i,k,1}, SK^2_{ID_i,k,1}) = (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}}, g_1^\alpha (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}})$ and $SK_{ID_i,k,2} = (SK^1_{ID_i,k,2}, SK^2_{ID_i,k,2}) = (R_1' g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}}, Q_1' g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}})$. It chooses randomly $\beta_{i,k+1}, \lambda_{i,k+1} \in Z_N$ and calculates a new private key:

$$SK_{ID_i,k+1} = (SK_{ID_i,k+1,1}, SK_{ID_i,k+1,2}),$$

where

$$\begin{aligned} SK_{ID_i,k+1,1} &= (SK^1_{ID_i,k,1} g_1^{\beta_{i,k+1}}, SK^2_{ID_i,k,1} g_1^{\gamma_{i,k+1}}) \\ &= (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} g_1^{\beta_{i,k+1}}, g_1^\alpha (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} g_1^{\gamma_{i,k+1}}) \\ &= (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}+\beta_{i,k+1}}, g_1^\alpha (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}+\gamma_{i,k+1}}) \end{aligned}$$

and

$$SK_{ID_i,k+1,2} = (SK^1_{ID_i,k,2} g_1^{-\beta_{i,k+1}}, SK^2_{ID_i,k,2} g_1^{-\gamma_{i,k+1}}) = (R'_1 g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}-\beta_{i,k+1}}, Q'_1 g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}-\gamma_{i,k+1}})$$

Since $\beta_{i,k+1}, \lambda_{i,k+1} \in Z_N$ are randomly selected, $\beta_{i,1} + \ldots + \beta_{i,k} + \beta_{i,k+1}$ and $\gamma_{i,1} + \ldots + \gamma_{i,k} + \gamma_{i,k+1}$ are also random. The private keys $SK_{ID_i,k+1}$ and $SK_{ID_i,k}$ have the same distributions. Without losing the generality, if a private key is needed, the original private key SK_{ID_i} will be used for the convenience.

Encryption algorithm. It takes M and one set $S = (ID_1, \ldots, ID_d)$ that will receive the ciphertext as the input. It randomly chooses $s \in Z_N$ and $Z, Z' \in G_{p_2}$ and computes the ciphertext:

$$CT = (C, Hdr) = (C, C_1, C_2) = (Me(g_1, g_1)^{\alpha s}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s Z, g_1^s Z')$$

The encapsulated key is $e(g_1, g_1)^{\alpha s}$. The data owner transmits (CT, S) to the receiver.

Decryption algorithm 1. For one user ID_i, if $ID_i \in S$, it can decrypt the received ciphertext. It divides $CT = (C, Hdr)$. They run the decryption algorithm **Decrypt**$1(MP, SK_{ID_i,k,1}, S, CT) \rightarrow CT'$. If $ID_i \in S$, the algorithm uses Hdr to calculate part of the plaintext, CT'.

First, it uses $SK_{ID_i,k,1}$ to calculate $CT' = (C, C_1, C_2, C'_1, C'_2)$:

$$C'_1 = e(SK^1_{ID_i,k,1}, C_1) = e(g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s Z),$$
$$C'_2 = e(SK^2_{ID_i,k,1}, C_2) = e(g_1^{\alpha} (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}}, g_1^s Z').$$

Decryption algorithm 2. The algorithm inputs MP, $SK_{ID_i,k,2}$, the user's identity set S and the part plaintext CT'. Supposing $ID_i \in S$, it first calculates the encapsulated key CK. Next, the plaintext message M is recovered by CK.

First, it calculates:

$$\begin{aligned} &C'_1 e(SK^1_{ID_i,k,2}, C_1) = e(SK^1_{ID_i,k,1}, C_1) e(SK^1_{ID_i,k,2}, C_1) \\ &= e(g_1^{r_i} R_1 R'_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s Z) \\ &= e(g_1^{r_i}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s) \end{aligned}$$

$$\begin{aligned} &C'_2 . e(SK^2_{ID_i,k,2}, C_2) = e(SK^2_{ID_i,k,1}, C_2)_2 . e(SK^2_{ID_i,k,2}, C_2) \\ &= e(g_1^{\alpha} (h \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 Q'_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}}, g_1^s Z') \\ &= e(g_1^{\alpha} (h \prod_{j=1}^{d} u_j^{ID_j})^{r_i}, g_1^s) \end{aligned}$$

Then, it obtains

$$M = C_0 \frac{C'_1 e(SK^1_{ID_i,k,2}, C_1)}{C'_2 . e(SK^2_{ID_i,k,2}, C_2)} = Me(g_1, g_1)^{\alpha s} \frac{e(g_1^{r_i}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s)}{e(g_1^{\alpha} (h \prod_{j=1}^{d} u_j^{ID_j})^{r_i}, g_1^s)} = M$$

For the semi-functional private key generation algorithm, given $SK_{ID_i,k} = (SK_{ID_i,k,1}, SK_{ID_i,k,2})$, where $SK_{ID_i,k,1} = (SK^1_{ID_i,k,1}, SK^2_{ID_i,k,1}) = (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}}, g_1^{\alpha} (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i}$

$Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}}$) and $SK_{ID_i,k,2}$= $(SK^1_{ID_i,k,2}, SK^2_{ID_i,k,2})$ =$(R'_1 g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}}, Q'_1 g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}})$, it randomly selects $\xi_1, \xi_2, \zeta_1, \zeta_2 \in Z_N$ and generates the semi-functional private key: $\widetilde{SK_{ID_i}} = \left(\widetilde{SK_{ID_i,k,1}}, \widetilde{SK_{ID_i,k,2}}\right)$, where $\widetilde{SK_{ID_i,k,1}} = (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} g_2^{\xi_1}, g_1^{\alpha}(h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i}$ $Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} g_2^{\xi_2}$) and $\widetilde{SK_{ID_i,k,2}} = (R'_1 g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}} g_2^{\zeta_1}, Q'_1 g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}} g_2^{\zeta_2})$.

The semi-functional encryption algorithm invokes **Encrypt** to gain normal ciphertext $CT = (C, Hdr) = (C, C_1, C_2) = (Me(g_1, g_1)^{\alpha s}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s Z, g_1^s Z')$.

Then, it randomly selects $\rho_1, \rho_2, \rho_3 \in Z_N$ and generates semi-functional ciphertexts:

$$\begin{aligned} \widetilde{CT} &= (\widetilde{C}, \widetilde{Hdr}) = (\widetilde{C}, \widetilde{C_1}, \widetilde{C_2}) = (C g_2^{\rho_1}, C_1 g_2^{\rho_2}, C_2 g_2^{\rho_3}) \\ &= (Me(g_1, g_1)^{\alpha s} g_2^{\rho_1}, (h_1 \prod_{j=1}^{d} u_j^{ID_j})^s Z g_2^{\rho_2}, g_1^s Z' g_2^{\rho_3}) \end{aligned}$$

6. Proof of Safety

Theorem 1. *Suppose that Assumption 1, Assumption 2 and Assumption 3 hold, and the leakage amount of the private key does not exceed* $L_{SK_1} = L_{SK_2} = (1 - 2\Lambda)\theta$ *bits, where* $\theta = \log_2^{w_2}$, *and* Λ *is a small constant number; the proposed CLR-SS-AIBBE scheme is CCA secure under the standard model, where* $L_{SK_1} = L_{SK_2} = L_{SK}$.

The main ideal of the proof. The indistinguishability of a series of games expounds its security of the given scheme. EX_R is a real security game, and the rest of the games are gradually changed from EX_R. In EX_F, any attacker has no advantage. As long as it is proven that the adversary cannot distinguish between two consecutive games, security is achieved. q denotes the maximum number of private key queries.

EX_R: It is the real security game of CLR-SS-AIBBE.

EX_0: It is very similar to EX_R. The only difference is that EX_0 has semi-functional ciphertext.

EX_i ($i \in [1, q]$): The challenger responds to $\mathcal{A}$ with a semi-functional ciphertext, responds to $\mathcal{A}$'s previous i private key inquiries with semi-functional ones and responds to the other private key queries with normal ones. Supposing $i = q$ (EX_q), the challenger generates semi-functional private keys to respond to all private key queries.

EX_F. The only difference between EX_q and EX_F is that in EX_F, $\mathcal{B}$ encrypts a message randomly, while in EX_q, $\mathcal{B}$ only encrypts one of the two given challenge messages.

Table 2 shows the types of the ciphertext and the private key for every game. The ciphertext or the private key represented by SMF is semi-functional. We use NM to indicate that one ciphertext or one private key is normal. The types for the ciphertext and the private key are represented by TY_{SK} and TY_{CT}, respectively. $\underbrace{((TY_{CT}, TY_{SK}), \ldots, (TY_{CT}, TY_{SK}))}_{q}$ indicates the corresponding type of the private keys and the ciphertexts of the q inquiries in one game. Since the ciphertext has the same form in every query, $\underbrace{((TY_{CT}, TY_{SK}), \ldots, (TY_{CT}, TY_{SK}))}_{q}$ can be abbreviated as $(TY_{CT}, \underbrace{TY_{SK}, \ldots, TY_{SK}}_{q})$.

Table 2. The forms of the ciphertext and the private key for every game (CLR-SS-AIBBE).

Game	Types of Ciphertext and Private Key (TY_{CT},TY_{SK},…,TY_{SK})
EX_R	(NM, NM, …, NM)
EX_0	(SMF, NM, …, NM)
EX_i $i \in (1, \ldots, q-1)$	$(\text{SMF}, \text{SMF}, \ldots, \underbrace{\text{SMF}}_{i+1}, \text{NM}, \ldots, \text{NM})$
EX_q	(SMF, SMF, …, SMF)
EX_F	(SMF, SMF, …, SMF)

Proof. We will complete the proof through EX_R, EX_i ($i \in (0, 1, \ldots, q)$) and EX_F and four lemmas. Lemma 1 gives the limit of leakage. The other three lemmas prove the indistinguishability of these games. Moreover, the advantage gained by the attacker in the game EX_F is proven to be negligible.

Table 3 illustrates the distinctions for the superiority achieved by the attacker between two consecutive games. Here, we give the conclusions of Lemma 2, Lemma 3 and Lemma 4. Their proofs will be given later. $Adv_{\mathcal{A}}^{EX_R}$ or $Adv_{\mathcal{A}}^{EX_R}(L_{SK})$ is used to indicate the superiority achieved by $\mathcal{A}$ in this game EX_R. We use $Adv_{\mathcal{A}}^{EX_i}$ or $Adv_{\mathcal{A}}^{EX_i}(L_{SK})$ to indicate the superiority achieved by $\mathcal{A}$ in this game EX_i ($i \in (0, \ldots, q)$). We use $Adv_{\mathcal{A}}^{EX_F}$ or $Adv_{\mathcal{A}}^{EX_F}(L_{SK})$ to indicate the superiority achieved by $\mathcal{A}$ in this game EX_F.

Table 3. The distinctions for the superiority achieved by the attacker between two consecutive games (CLR-SS-AIBBE).

Two Consecutive Games	Differences of the Advantages	Lemmas
EX_R or EX_0	$\left\|Adv_{\mathcal{A}}^{EX_R} - Adv_{\mathcal{A}}^{EX_0}\right\| \leq \varepsilon$	Lemma 2
EX_i or EX_{i-1} $i \in (1, \ldots, q)$	$\left\|Adv_{\mathcal{A}}^{EX_{i-1}} - Adv_{\mathcal{A}}^{EX_i}\right\| \leq \varepsilon$	Lemma 3
EX_q or EX_F	$\left\|Adv_{\mathcal{A}}^{EX_q} - Adv_{\mathcal{A}}^{EX_F}\right\| \leq \varepsilon$	Lemma 4

From Table 3, the following fact can be obtained.

$$\begin{aligned}
&\left|Adv_{\mathcal{A}}^{EX_R} - Adv_{\mathcal{A}}^{EX_F}\right| \\
=&\left|Adv_{\mathcal{A}}^{EX_R} - Adv_{\mathcal{A}}^{EX_0} + Adv_{\mathcal{A}}^{EX_0} - \ldots - Adv_{\mathcal{A}}^{EX_i} + Adv_{\mathcal{A}}^{EX_i} - \cdots\right. \\
&\left. - Adv_{\mathcal{A}}^{EX_q} + Adv_{\mathcal{A}}^{EX_q} - Adv_{\mathcal{A}}^{EX_F}\right| \\
\leq& \left|Adv_{\mathcal{A}}^{EX_R} - Adv_{\mathcal{A}}^{EX_0}\right| + \left|Adv_{\mathcal{A}}^{EX_0} - Adv_{\mathcal{A}}^{EX_1}\right| + \ldots + \left|Adv_{\mathcal{A}}^{EX_q} - Adv_{\mathcal{A}}^{EX_F}\right| \\
\leq& (q+2)\varepsilon
\end{aligned}$$

So, $\left|Adv_{\mathcal{A}}^{EX_R} - Adv_{\mathcal{A}}^{EX_F}\right| \leq (q+2)\varepsilon$. Furthermore, according to theorem 6.8 given in [50], we obtain that $Adv_{\mathcal{A}}^{EX_F} \leq \varepsilon$. Thus, the proof of Theorem 1 is completed.

Lemma 1. *The maximum amount of one private key leakage can reach* $L_{SK_1} = L_{SK_2} = (1 - 2\Lambda)\theta$.

Proof. We will utilize a result in ref. [26] to complete the proof.

Result 1 ([26]). *Given a prime p, we select* $n_1 \geq n_2 \geq 2$ $(n_1, n_2 \in N)$, *a matrix* $X \leftarrow Z_p^{n_1 \times n_2}$ *and a matrix* $Y \leftarrow Rk_1(Z_p^{n_2 \times 1})$, *with rank 1 and* $\Theta \leftarrow Z_p^{n_1}$. *The leakage function is* $f : Z_p^{n_1} \rightarrow W$. *As long as* $\left|W\right| \leq 4 \cdot (1 - \frac{1}{p}) \cdot p^{n_2 - 1} \cdot \varepsilon^2$, *the statistical distance* $SD((X, f(X \cdot Y)), (X, f(\Theta)) \leq \varepsilon$, *where* ε *is a negligible value.*

According to Result 1, the following Deduction 1 is obtained easily.

Deduction 1. *Given a prime p, we choose $n_1 \geq 3$, $\vec{\delta} \leftarrow Z_p^{n_1}$, $\vec{\tau} \leftarrow Z_p^{n_1}$ and $\vec{\tau}' \leftarrow Z_p^{n_1}$ such that the dot product of $\vec{\tau}'$ and $\vec{\delta}$ is orthogonal with respect to the module p. Suppose that the leakage function is $f : Z_p^{n_1} \to W$. As long as $\left|W\right| \leq 4 \cdot (1 - \frac{1}{p}) \cdot p^{n_1-2} \cdot \varepsilon^2$, $SD((\vec{\delta}, f(\vec{\tau}')), (\vec{\delta}, f(\vec{\tau}))) \leq \varepsilon$.*

Proof. According to the conclusion 1, if $n_2 = n_1 - 1$, $n_1 = n_2 + 1 \geq n_2 \geq 2$. This basis of the orthogonal space of $\vec{\delta}$ corresponds to X and $\vec{\tau}$ corresponds to Φ. So, when $Y \leftarrow Rk_1(Z_p^{(n_1-1)\times 1})$, the distributions of $\vec{\tau}'$ are the same as $X \cdot Y$. Since $\vec{\delta}$ is randomly selected, $X \leftarrow Z_p^{n_1 \times (n_1-1)}$ is uniquely determined by $\vec{\delta}$. According to Deduction 1, we obtain $SD((\vec{\delta}, f(\vec{\tau}')), (\vec{\delta}, f(\vec{\tau}))) = dist((X, f(X \cdot T)), (X, f(\Phi))$. □

If we set $n_2 = 2$, $p_2 = p$ and $\varepsilon = p_2^{-\Lambda}$, the allowed value of private key leakage is $\log_2^{|W|} \leq (2-1)\log_2^{w_2} - 2\Lambda \log_2^{w_2} = (1 - 2\Lambda)\log_2^{w_2} = (1 - 2\Lambda)\theta$, where $\log_2^{w_2} = \theta$. Thus, the maximum value of private key leakage can reach $L_{SK_1} = L_{SK_2} = L_{SK} = (1 - 2\Lambda)\theta$. □

Lemma 2. *If there is an adversary $\mathcal{A}$, such that $\left|Adv_{\mathcal{A}}^{\mathrm{EX_R}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_0}}(L_{SK})\right| \geq \varepsilon$, the challenger $\mathcal{B}$ can destroy Assumption 1 over advantage ε.*

Proof. Given $D = (\Omega, g_1, X_3)$, $U, V \in G_{w_2}$ and T ($T \in G_{w_1 w_2}$ or $T \in G_{w_1}$), $\mathcal{B}$ and $\mathcal{A}$ interact as follows.

Initialization. Let l indicate the maximum number of users. The challenger $\mathcal{B}$ randomly selects $g_1, h_1 \in G_{w_1}, g_3 \in G_{w_3}$, $a_1, a_2, \ldots, a_l, b \in Z_N$ and $\alpha \in Z_N$. $\mathcal{B}$ sets $u_1 = g_1^{a_1}, \ldots, u_l = g_1^{a_l}$ and $h_1 = g_1^b$.

The master public key is $MP = \left\{N, g_1, g_3, h_1, u_1, \ldots, u_l, e(g_1, g_1)^{\alpha}\right\}$, and the master private key is $MK = \{\alpha\}$. $\mathcal{B}$ sends MP to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ inquires the private key of $ID_i \in S$, where $S = (ID_1, \ldots, ID_d)$, $(d \leq l)$ is this set of the intended recipients, $\mathcal{B}$ randomly selects $\beta_{i,0}, \gamma_{i,0} \in Z_N$ and $r_i \in Z_N (i = \{1, \ldots, d\}) r_i, q_i, r_i', q_i' \in Z_N$. $\mathcal{B}$ generates private key $SK_{ID_i,0} = \left(SK_{ID_i,0,1}, SK_{ID_i,0,2}\right)$, where $SK_{ID_i,0,1} = (g_1^{r_i} X_3^{r_i} g_1^{\beta_{i,0}}, g_1^{\alpha}(h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} X_3^{q_i} g_1^{\gamma_{i,0}})$ and $SK_{ID_i,0,2} = (g_1^{-\beta_{i,0}} X_3^{r_i'}, g_1^{-\gamma_{i,0}} X_3^{q_i'})$. $\mathcal{B}$ responds to $\mathcal{A}$ with the private key SK_{D_i}.

Challenge. $\mathcal{A}$ gives $\mathcal{B}$ one set $S^* = \left\{ID_1^*, \ldots, D_d^*\right\}$ and two messages, M_0 and M_1, of equal size. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and calculates ciphertext $CT = (C, Hdr) = (C, C_1, C_2) = (Me(g_1, T)^{\alpha}, T^{\sum_{j=1}^{d} a_j ID_j + b} U, TV)$.

Phase 2. $\mathcal{A}$ may query the private key for $ID_i \notin S^*$.

Guess. $\mathcal{A}$ output a guess β'. If β', $\mathcal{A}$ wins the game.

When $T = g_1^z g_2^v \in G_{w_1 w_2}$ (z, v are randomly selected), $\mathcal{B}$ properly simulates the game $\mathrm{EX_0}$. When $T = g_1^z \in G_{w_1}$ (z is randomly selected), $\mathcal{B}$ properly simulates the game $\mathrm{EX_R}$. In other words, as long as $\mathcal{A}$ achieves certain advantages in distinguishing $\mathrm{EX_R}$ and $\mathrm{EX_0}$, the challenger has the same advantages in destroying assumption 1. This is not consistent with Assumption 1. So, $\left|Adv_{\mathcal{A}}^{\mathrm{EX_R}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_0}}(L_{SK})\right| < \varepsilon$. □

Lemma 3. *If there is an adversary $\mathcal{A}$ such that $\left|Adv_{\mathcal{A}}^{\mathrm{EX_{k-1}}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK})\right| \geq \varepsilon$ ($k \in (1, \ldots, q)$), the challenger $\mathcal{B}$ can destroy Assumption 2 over advantage ε.*

Proof. Given $D = (\Omega, g_1, X_1 X_2, X_3, Y_2 Y_3)$ and T ($T \in G_{w_1 w_3}$ or $T \in G_1$), $\mathcal{B}$ and $\mathcal{A}$ interact as follows.

Initialization. Let l indicate the maximum number of users. The challenger $\mathcal{B}$ randomly selects $g_1, h_1 \in G_{w_1}, g_3 \in G_{w_3}$, $a_1, a_2, \ldots, a_l, b \in Z_N$ and $\alpha \in Z_N$. $\mathcal{B}$ sets $u_1 = g_1^{a_1}, \ldots, u_l = g_1^{a_l}$ and $h_1 = g_1^b$.

The master public key is $MP = \left\{N, g_1, g_3, h_1, u_1, \ldots, u_l, e(g_1, g_1)^\alpha\right\}$, and the master private key is $MK = \{\alpha\}$. $\mathcal{B}$ sends MP to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ inquires a private key, which corresponds to $ID_i \in S$, where $S = \{ID_1, \ldots, ID_d\}$. $\mathcal{B}$ responds like this.

(1) In case $i < k$, $\mathcal{B}$ responds with one private key with a semi-functional form. $\mathcal{B}$ randomly picks $\xi_1, \xi_2, \zeta_1, \zeta_2 \in Z_N$ and generates one private key with the semi-functional form $\widetilde{SK_{ID_i}} = \left(\widetilde{SK_{ID_i,k,1}}, \widetilde{SK_{ID_i,k,2}}\right)$, where

$\widetilde{SK_{ID_i,k,1}} = (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} (g_2^u g_3^\varsigma)^{\xi_1}, g_1^\alpha (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} (g_2^u g_3^\varsigma)^{\xi_2})$ and

$\widetilde{SK_{ID_i,k,2}} = (R_1' g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}} (g_2^u g_3^\varsigma)^{\zeta_1}, Q_1' g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}} (g_2^u g_3^\varsigma)^{\zeta_2})$.

(2) In case $i > k$, $\mathcal{B}$ calls the private key generation algorithm to gain one private key with normal form.

(3) In case $i = k$, $\mathcal{B}$ randomly picks $\beta_{i,k}, \gamma_{i,k} \in Z_N$, $r_i \in Z_N (i = \{1, \ldots, d\})$ and $R_i, Q_i, R_i', Q_i' \in G_{p_3}$. $\mathcal{B}$ generates a private key $SK_{ID_i,k} = \left(SK_{ID_i,k,1}, SK_{ID_i,k,2}\right)$, where

$SK_{ID_i,k,1} = (SK^1_{ID_i,k,1}, SK^2_{ID_i,k,1}) = (T^{r_i} g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} R_1, g_1^\alpha (T^{\sum_{j=1}^{d} a_j ID_j + b})^{r_i} g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} Q_1)$ and

$SK_{ID_i,k,2}(SK^1_{ID_i,k,2}, SK^2_{ID_i,k,2}) = (R_1' g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}}, Q_1' g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}})$.

Provided $T \in G_{w_1 w_3}$, this private key is normal. $\mathcal{B}$ correctly imitates $\mathrm{EX_{k-1}}$.

Provided $T \in G_1$, this private key has a semi-functional form. $\mathcal{B}$ correctly imitates $\mathrm{EX_k}$.

Challenge. $\mathcal{A}$ gives $\mathcal{B}$ one set $S^* = \left\{ID_1^*, \ldots, D_d^*\right\}$ and two messages, M_0 and M_1, of equal size. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and calculates ciphertext

$$CT = (C, Hdr) = (C, C_1, C_2) = (M_\beta e(g_1, g_1^z g_2^v)^\alpha, (g_1^z g_2^v)^{\sum_{j=1}^{d} a_j ID_j^* + b}, g_1^z g_2^v)$$

Phase 2. $\mathcal{A}$ may query the private key for $ID_i \notin S^*$.

Guess. $\mathcal{A}$ output a guess β'. If $\beta' = \beta$, $\mathcal{A}$ wins the game.

When $T \in G_{w_1 w_3}$, $\mathcal{B}$ properly simulates the game $\mathrm{EX_{k-1}}$. When $T \in G_1$, $\mathcal{B}$ properly simulates the game $\mathrm{EX_k}$. Thus, $|\Pr[\mathcal{B}(D, T \in G_{w_1 w_3}) = 0] - \mathcal{B}(D, T \in G_1) = 0]| = |Adv_{\mathcal{A}}^{\mathrm{EX_{k-1}}} - Adv_{\mathcal{A}}^{\mathrm{EX_k}}| \geq \varepsilon$. In other words, as long as $\mathcal{A}$ achieves certain advantages in distinguishing $\mathrm{EX_{k-1}}$ and $\mathrm{EX_k}$, the challenger has the same advantages in destroying Assumption 2. This is not consistent with assumption 2. So, $\left|Adv_{\mathcal{A}}^{\mathrm{EX_{k-1}}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK})\right| < \varepsilon$.

For the same reason, as for $i \in [k, q]$, $\left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_{k+1}}}(L_{SK})\right| < \varepsilon$, ... , and $\left|Adv_{\mathcal{A}}^{\mathrm{EX_{q-1}}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK})\right| < \varepsilon$. So,

$$\begin{aligned}
&\left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK})\right| \\
=&\left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_{k+1}}}(L_{SK}) + \ldots + Adv_{\mathcal{A}}^{\mathrm{EX_{q-1}}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK})\right| \\
<&\left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_{k+1}}}(L_{SK})\right| + \ldots + \left|Adv_{\mathcal{A}}^{\mathrm{EX_{q-1}}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK})\right| \\
<&(q-k)\varepsilon
\end{aligned}$$

In addition, $\left|Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_F}}(L_{SK})\right| < \varepsilon$ (the proof will be given in Lemma 4). In this way, we can obtain:

$$\begin{aligned} & Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) \\ = & \left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) + Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_F}}(L_{SK})\right| \\ < & \left|Adv_{\mathcal{A}}^{\mathrm{EX_k}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK})\right| + \left|Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_F}}(L_{SK})\right| \\ < & (q-k+1)\varepsilon \end{aligned}$$

In other words, the advantage gained by $\mathcal{A}$ in $\mathrm{EX_i}$ can be ignored. Lemma 3 is finished. □

Lemma 4. *If there is an adversary $\mathcal{A}$ such that $\left|Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_F}}(L_{SK})\right| \geq \varepsilon$, the challenger $\mathcal{B}$ can destroy assumption 3 over advantage ε.*

Proof. Given $D = (\Omega, g_1, g_1^{\alpha} X_2, X_3, g_1^{s} Y_2, Z_2)$ and T ($T = e(g_1, g_1)^{\alpha s}$ or $T \in G_2$, where $s \in Z_N$ is randomly selected), $\mathcal{B}$ and $\mathcal{A}$ interact as follows.

Initialization. Let l indicate the maximum number of users. The challenger $\mathcal{B}$ randomly selects $g_1, h_1 \in G_{w_1}, g_3 \in G_{w_3}$, $a_1, a_2, \ldots, a_l, b \in Z_N$ and $\alpha \in Z_N$. $\mathcal{B}$ sets $u_1 = g_1^{a_1}, \ldots, u_l = g_1^{a_l}$ and $h_1 = g_1^{b}$.

The master public key is $MP = \left\{N, g_1, g_3, h_1, u_1, \ldots, u_l, e(g_1, g_1)^{\alpha}\right\}$, and the master private key is $MK = \{\alpha\}$. $\mathcal{B}$ sends MP to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ queries the private key that corresponds to the identity $ID_i \in S$, where $S = \{ID_1, \ldots, ID_d\}$. $\mathcal{B}$ randomly selects $\xi_1, \xi_2, \zeta_1, \zeta_2 \in Z_N$ and generates one private key with the semi-functional form $\widetilde{SK_{ID_i}} = \left(\widetilde{SK_{ID_i,k,1}}, \widetilde{SK_{ID_i,k,2}}\right)$, where $\widetilde{SK_{ID_i,k,1}} = (g_1^{r_i} R_1 g_1^{\beta_{i,1}+\ldots+\beta_{i,k}} (g_2^u g_3^{\zeta})^{\xi_1}, g_1^{\alpha} (h_1 \prod_{j=1}^{d} u_j^{ID_j})^{r_i} Q_1 g_1^{\gamma_{i,1}+\ldots+\gamma_{i,k}} (g_2^u g_3^{\zeta})^{\xi_2})$ and $\widetilde{SK_{ID_i,k,2}} = (R_1' g_1^{-\beta_{i,1}-\ldots-\beta_{i,k}} (g_2^u g_3^{\zeta})^{\zeta_1}, Q_1' g_1^{-\gamma_{i,1}-\ldots-\gamma_{i,k}} (g_2^u g_3^{\zeta})^{\zeta_2})$.

Challenge. $\mathcal{A}$ gives $\mathcal{B}$ one set $S^* = \left\{ID_1^*, \ldots, D_d^*\right\}$ and two messages, M_0 and M_1, of equal size. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and calculates ciphertext

$$\widetilde{CT} = (C, Hdr) = (C, C_1, C_2) = (M_{\beta} T, (g_1^{s} g_2^{u})^{\sum_{i=1}^{d} a_i ID_i^* + b} Z, g_1^{s} g_2^{u} Z')$$

Phase 2. $\mathcal{A}$ may query the private key for $ID_i \notin S^*$.

Guess. $\mathcal{A}$ output a guess β'. If β', $\mathcal{A}$ wins the game.

When $T = e(g_1, g_1)^{\alpha s}$, $\mathcal{B}$ properly simulates the game $\mathrm{EX_q}$. When $T \in G_2$, $\mathcal{B}$ properly simulates the game $\mathrm{EX_F}$. Thus, $|\Pr[\mathcal{B}(D, T = e(g_1, g_1)^{\alpha s}) = 0] - \mathcal{B}(D, T \in G_2) = 0]| = |Adv_{\mathcal{A}}^{\mathrm{EX_q}} - Adv_{\mathcal{A}}^{\mathrm{EX_F}}| \geq \varepsilon$. In other words, as long as $\mathcal{A}$ achieves certain advantages in distinguishing $\mathrm{EX_q}$ and $\mathrm{EX_F}$, the challenger has the same advantages in destroying Assumption 3. This is not consistent with Assumption 3. So, $\left|Adv_{\mathcal{A}}^{\mathrm{EX_q}}(L_{SK}) - Adv_{\mathcal{A}}^{\mathrm{EX_F}}(L_{SK})\right| < \varepsilon$. □ □

As time goes on the leakage must exceed a certain limit, which will damage the security of the system. If the scheme keeps secure against continual side-channel attack, its private key should be refreshed periodically. In fact, through the update algorithm for the private key, our scheme has the function of continual-leakage resilience.

Theorem 2. *The scheme of CLR-SS-AIBBE has continual-leakage resilience.*

Proof. Similar to [52], the proposed CLR-SS-AIBBE gains continual leakage resilience through the update algorithm for the private key. The private key updation algorithm inputs $SK_{ID,k}$ and MP and generates one new private key $SK_{ID,k+1}$. For the private key updation, an additional random number is added to the original one of the private key.

Since the newly added value is randomly selected, the new private key has the same distribution with the original one. If private key updates periodically, continual-leakage resilience can be obtained. □

7. Relative Leakage Ratio

The relative leakage ratio of one private key refers to the ratio of the leakage amount of one private key to the length of the private key.

In our proposed scheme, w_1, w_2 and w_3 are primes with length of θ bits. This private key has $2 \times 2 \times 3\theta$ bits. The leakage amount of the private key amounts to $2 \times 2(1 - 2\Lambda)\theta$ bits, where Λ is a very small constant value. So, the relative leakage ratio about the private key is $\frac{4(1-2\Lambda)\theta}{12\theta} = \frac{4(1-2\Lambda)}{12} \approx \frac{1}{3}$.

Table 4 shows some comparisons about the proposed scheme and some related schemes are given in [51,53]. We will consider the private key size, leakage amount, storage requirement and leakage rate. Ref. [53] gives an anonymous IBBE scheme but does not consider leakage. Ref. [51] proposes a continuous-leakage-resilient (CLR) IBBE scheme (CLR-IBBE), which essentially uses the private key extension technology, but does not consider the anonymity. The scheme given in this paper takes account of both key leakage and anonymity.

Table 4. Some comparisons related to the proposed scheme and some related schemes given in [51,53].

Schemes	IBBE of [53]	CLR-IBBE of [51]	Our Scheme
Private key size	6θ	$3(n+2)\lambda$	12θ
Leakage amount of SK	$\times$	$(n - 2\Lambda - 1)\lambda$	$4(1 - 2\Lambda)\theta$
Storage requirement	2	$n + 2$	4
Private updation	$\times$	$\surd$	$\surd$
Leakage rate of SK	0	$\frac{(n-2\Lambda-1)}{3(n+2)}$	$\frac{4(1-2\Lambda)}{12} \approx \frac{1}{3}$
CLR	$\times$	$\surd$	$\surd$
Split-state	$\times$	$\times$	$\surd$
Anonymity	$\surd$	$\times$	$\surd$

From Table 4, we see that the leakage resilience of the given scheme is better than that of [51]. In addition, because the scheme of [51] requires $n \geq 2$, the storage requirement of our scheme is better than that of [51]. In fact, for the scheme of [51], when n is a large value, a high leakage rate can be obtained. For example, when $n = 2$, the private key leakage ratio in [51] is $\frac{1}{12}$. When $n = 4$, the private key leakage ratio of the scheme [51] is $\frac{1}{6}$. The leakage rate of the scheme in [51] increases with the increase in n, but the maximum leakage rate is $\frac{1}{3}$. The essence is that the scheme of [51] obtains certain leakage resilience at the expense of storage space and calculation cost. The scheme of this paper divides the private key into two different states through state partition technology, so that the private key can be properly separated to obtain leakage resilience.

8. Comparisons of Calculation Efficiency

Table 5 shows the comparisons of the calculation efficiency of our scheme and the schemes of [51,53].

Table 5. Comparisons of the calculation efficiency of our scheme and the schemes of [51,53].

Schemes	Initialization	Private Generation	Private Updation	Encryption	Decryption
[53]	$E + P$	$(d+2)E$	$\times$	$(d+3)E$	$2P$
[51]	$(4n+3m+5)E+P$	$(3n+2d+4)E$	$(3n+d+5)E$	$(n+d+2)E$	$(n+2)P$
Our scheme	$E + P$	$(d+4)E$	$4E$	$(d+3)E$	$4P$

The number of main operations (pairing operation and group exponent operation) is listed in Table 5. *P* indicates pairing operation. *E* indicates group exponent operation. *m* is the max value of the users in the system. *d* denotes the count of those users in some broadcast. The calculation efficiency of each operation of this presented scheme in this paper is better than that of the scheme in [51]. The encryption and decryption calculation efficiency of our scheme is as good as that of [53], and the efficiency is higher than that of the scheme in [51]. Since the private key is divided into two states, the scheme in this paper has two more exponential operations than the scheme in [53] for the private key generation algorithm. In addition, since the decryption is divided into two stages, the scheme in this paper has two more pairing operations than the scheme in [53].

9. Conclusions

This paper gives the syntax and security description of CLR-SS-AIBBE and proposes a concrete CLR-SS-AIBBE scheme. The private key is continuously updated through state division. The proposed scheme can resist the continual leakage about the private key. The relative leakage rate reaches one-third. Based on the general subgroup decision hypothesis, it is proven that our scheme is secure under the standard model. In addition, through the special treatment of a private key, this given scheme also has the characteristics of anonymity. It has three advantages.

First, our scheme has better application value. Since the adversary in the real environment can carry out continuous-leakage attacks, the continuous-leakage model is closer to the application needs of the real environment. In this paper, the leakage-resilient performance of IBBE mechanism is achieved under the continuous-leakage model, so the scheme is more practical.

Second, our scheme has better user-identity privacy protection. In the identity-based broadcast encryption scheme, broadcasters usually encrypt messages by combining the public identity of the receiver and system parameters. This may reveal the identity of the receiver to the public, which causes users to worry about identity privacy. Most identity-based broadcast encryption (IBBE) schemes are not anonymous, which means that attackers can obtain the identities of all recipients from the ciphertext. The paper provides anonymity and has a good role in protecting user identity privacy.

Third, the given scheme is suitable for some intelligent systems. The public parameter size and private key size of the proposed scheme are constant, and the decryption cost is independent of the number of recipients. Therefore, this scheme requires less computing energy consumption and is very suitable for intelligent city information systems.

Author Contributions: Conceptualization and methodology, Q.Y. and J.L.; formal analysis, Q.Y. and S.J.; writing—original draft preparation, Q.Y.; writing—review and editing, Q.Y. and S.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Ref. 62172292, 62072104, 61972095, U21A20465).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kumar, S.; Dasu, V.A.; Baksi, A.; Sarkar, S.; Jap, D.; Breier, J.; Bhasin, S. Side Channel attack on stream giphers: A three-step approach to state/key recovery. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2022**, *2022*, 166–191. [CrossRef]
2. Won, Y.S.; Chatterjee, S.; Jap, D.; Basu, A.; Bhasin, S. WaC: First results on practical side-channel attacks on commercial machine learning accelerator. SIGSAC. In Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security, Virtual Event, Korea, 19 November 2021.

3. Das, D.; Ghosh, S.; Raychowdhury, A.; Sen, S. EM/Power side-channel attack: White-box modeling and signature attenuation countermeasures. *IEEE Des. Test.* **2021**, *38*, 67–75. [CrossRef]
4. Won, Y.S.; Chatterjee, S.; Jap, D.; Bhasin, S.; Basu, A. Time to leak: Cross-device timing attack on edge deep learning accelerator. In Proceedings of the 2021 International Conference on Electronics, Information, and Communication (ICEIC), Jeju, Korea, 31 January–3 February 2021.
5. Goldwasser, S.; Micali, S. Probabilistic encryption. *J. Comput. Syst. Sci.* **1984**, *28*, 270–299. [CrossRef]
6. Goldwasser, S.; Micali, S.; Rivest, R.L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **1988**, *17*, 281–308. [CrossRef]
7. Goldreich, O.; Micali, S.; Wigderson, A. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM* **1991**, *38*, 691–729. [CrossRef]
8. Agrawal, D.; Archambeault, B.; Rao, J.R.; Rohatgi, P. The EM side-channel(s). In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2002, Redwood Shores, CA, USA, 13–15 August 2003.
9. Halderman, J.A.; Schoen, S.D.; Heninger, N.; Clarkson, W.; Paul, W.; Calandrino, J.A.; Feldman, A.J.; Felten, J.A.; Appelbaum, J.; Felten, E.W. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM* **2009**, *52*, 91–98. [CrossRef]
10. Lipp, M.; Schwarz, M.; Gruss, D.; Prescher, T.; Haas, W.; Horn, J.; Mangard, S.; Kocher, P.; Genkin, D.; Yarom, Y.; et al. Meltdown: Reading kernel memory from user space. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17August 2018.
11. Kocher, P.; Horn, J.; Fogh, A.; Genkin, D.; Gruss, D.; Haas, W.; Hamburg, M.; Lipp, M.; Mangard, S.; Prescher, T.; et al. Spectre Attacks: Exploiting Speculative execution. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 13–19 May 2019.
12. Micali, S.; Reyzin, L. Physically observable cryptography. In Proceedings of the Theory of Cryptography Conference, Cambridge, MA, USA, 19–21 February 2004.
13. Dziembowski, S.; Pietrzak, K. Leakage-resilient cryptography. In Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science, Philadelphia, PA, USA, 25–28 October 2008.
14. Goldwasser, S.; Kalai, Y.T.; Rothblum, G.N. One-time programs. In Proceedings of the 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2008.
15. Akavia, A.; Goldwasser, S.; Vaikuntanathan, V. Simultaneous hardcore bits and cryptography against memory attacks. In Proceedings of the Theory of Cryptography Conference, San Francisco, CA, USA, 15–17 March 2009.
16. Naor, M.; Segev, G. Public-key cryptosystems resilient to key leakage. *SIAM J. Comput.* **2012**, *41*, 772–814. [CrossRef]
17. Luo, X.; Qian, P.; Zhu, Y. Leakage-resilient IBE from lattices in the standard model. In Proceedings of the 2nd International Conference on Information Science and Engineering, Hangzhou, China, 4–6 December 2010.
18. Li, S.; Zhang, F.; Sun, Y.; Shen, L. A new variant of the Cramer-Shoup leakage-resilient public key encryption. In Proceedings of the 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, Bucharest, Romania, 19–21 September 2012.
19. Chen, Y.; Zhang, Z.; Lin, D.; Cao, Z. Generalized (identity-based) hash proof system and its applications. *Secur. Commun. Netw.* **2016**, *9*, 1698–1716. [CrossRef]
20. Li, J.; Teng, M.; Zhang, Y.; Yu, Q. A leakage-resilient CCA-Secure identity-based encryption scheme. *Comput. J.* **2016**, *59*, 1066–1075. [CrossRef]
21. Prouff, E.; Rivain, M. Masking against side-channel attacks: A formal security proof. In Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 26–30 May 2013.
22. Duc, A.; Dziembowski, S.; Faust, S. Unifying leakage models: From probing attacks to noisy leakage. *J. Cryptol.* **2019**, *32*, 151–177. [CrossRef]
23. Hazay, C.; Lopez-Alt, A.; Wee, H. Leakage-resilient cryptography from minimal assumptions. *J. Cryptol.* **2016**, *29*, 514–551. [CrossRef]
24. Galindo, D.; Großschädl, J.; Liu, Z.; Vadnala, P.K.; Vivek, S. Implementation of a leakage-resilient ElGamal key encapsulation mechanism. *J. Cryptogr. Eng.* **2016**, *6*, 229–238. [CrossRef]
25. Genkin, D.; Ishai, Y.; Weiss, M. How to construct a leakage-resilient (stateless) trusted party. In Proceedings of the 15th International Conference, TCC 2017, Baltimore, MD, USA, 12–15 November 2017.
26. Brakerski, Z.; Kalai, Y.T.; Katz, J.; Vaikuntanathan, V. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In Proceedings of the Foundations of Computer Science (FOCS 2010), Las Vegas, NV, USA, 23–26 October 2010.
27. Dodis YDodis, Y.; Haralambiev, K.; López-Alt, A.; Wichs, D. Cryptography against continuous memory attacks. In Proceedings of the Foundations of Computer Science (FOCS 2010), Las Vegas, NV, USA, 23–26 October 2010.
28. Xiong, H.; Zhang, C.; Yuen, T.H.; Zhang, E.P.; Yiu, S.M.; Qing, S. Continual leakage-resilient dynamic secret sharing in the split-state model. In Proceedings of the 14th International Conference on Information and Communications Security, ICICS 2012, Hong Kong, China, 29–31 October 2012.
29. Li, J.; Yu, Q.; Zhang, Y. Hierarchical Attribute Based Encryption with Continuous Leakage-Resilience. *Inf. Sci.* **2019**, *484*, 113–134. [CrossRef]

30. Fiat, A.; Naor, M. Broadcast encryption. In Proceedings of the 13th Annual International Cryptology Conference, Santa Barbara, CA, USA, 22–26 August 1993.
31. Chen, L.; Li, J.; Zhang, Y. Adaptively secure efficient broadcast encryption with constant-size secret keys and ciphertext. *Soft Comput.* **2020**, *24*, 4589–4606. [CrossRef]
32. Chen, L.; Li, J.; Lu, Y.; Zhang, Y. Adaptively secure certificate-based broadcast encryption and its application to cloud storage service. *Inf. Sci.* **2020**, *538*, 273–289. [CrossRef]
33. Chen, L.; Li, J.; Zhang, Y. Anonymous certificate-based broadcast encryption with personalized messages. *IEEE Trans. Broadcast.* **2020**, *66*, 867–881. [CrossRef]
34. Zhong, H.; Zhang, S.; Cui, J.; Wei, L.; Liu, L. Broadcast encryption scheme for V2I communication in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *71*, 2749–2760. [CrossRef]
35. Delerablée, C. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007.
36. Ren, Y.; Gu, D. Fully CCA2 secure identity based broadcast encryption without random oracles. *Inf. Process. Lett.* **2009**, *109*, 527–533. [CrossRef]
37. Zhang, L.; Hu, Y.; Wu, Q. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. *Math. Comput. Model.* **2012**, *55*, 12–18. [CrossRef]
38. Libert, B.; Paterson, K.G.; Quaglia, E.A. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012.
39. Zhang, L.; Wu, Q.; Mu, Y. Anonymous identity-based broadcast encryption with adaptive security. In Proceedings of the 5th International Symposium, CSS 2013, Zhangjiajie, China, 13–15 November 2013.
40. Li, J.; Chen, L.; Lu, Y.; Zhang, Y. Anonymous certificate-based broadcast encryption with constant decryption cost. *Inf. Sci.* **2018**, *454*, 110–127. [CrossRef]
41. Lai, J.; Mu, Y.; Guo, F.; Jiang, P.; Ma, S. Identity-Based Broadcast Encryption for Inner Products. *Comput. J.* **2018**, *61*, 1240–1251. [CrossRef]
42. Jiang, P.; Guo, F.; Mu, Y. Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. *Theor. Comput. Sci.* **2019**, *767*, 51–72. [CrossRef]
43. Zhao, Z.; Guo, F.; Lai, J.; Susilo, W.; Wang, B.; Hu, Y. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. *Theor. Comput. Sci.* **2020**, *809*, 73–87. [CrossRef]
44. Chen, L.; Li, J.; Zhang, Y. Adaptively secure anonymous identity-based broadcast encryption for data access control in cloud storage service. *KSII Trans. Internet Inf. Syst.* **2019**, *13*, 1523–1545.
45. Liu, F.H.; Lysyanskaya, A. Tamper and leakage resilience in the split-state model. In Proceedings of the 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012.
46. Faonio, A.; Nielsen, J.B.; Simkin, M.; Venturi, D. Continuously non-malleable codes with split-state refresh. *Theor. Comput. Sci.* **2019**, *759*, 98–132. [CrossRef]
47. Aggarwal, D.; Döttling, N.; Nielsen, J.B.; Obremski, M.; Purwanto, E. Continuous non-malleable codes in the 8-split-state model. In Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 19–23 May 2019.
48. Kanukurthi, B.; Obbattu, S.A.I.; Lakshmi, B.; Sekar, S. Four-state non-malleable codes with explicit constant rate. *J. Cryptol.* **2020**, *33*, 1044–1079. [CrossRef]
49. Waters, B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Proceedings of the Advances in Cryptology-CRYPTO2009, Santa Barbara, CA, USA, 16–20 August 2009.
50. Lewko, A.; Rouselakis, Y.; Waters, B. Achieving leakage resilience through dual system encryption. In Proceedings of the 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, 28–30 March 2011.
51. Li, J.; Yu, Q.; Zhang, Y. Identity-based broadcast encryption with continuous leakage resilience. *Inf. Sci.* **2018**, *429*, 177–193. [CrossRef]
52. Li, J.; Guo, Y.; Yu, Q.; Lu, Y.; Zhang, Y. Provably secure identity-based encryption resilient to post-challenge continuous auxiliary inputs leakage. *Secur. Commun. Netw.* **2016**, *9*, 1016–1024. [CrossRef]
53. Ming, Y.; Yuan, H.; Sun, B.; Qiao, Z. Efficient identity-based anonymous broadcast encryption scheme in standard model. *J. Comput. Appl.* **2016**, *36*, 2762–2766.
54. Boneh, D.; Goh, E.; Nissim, K. Evaluating 2-DNF formulas on ciphertexts. In Proceedings of the Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, 10–12 February 2005.