Proceedings of CECNet 2021
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA210432

A New Identity-Based Encryption Scheme with Accountable Authority Based on SM9

Ke WANG [a,b], Yuan ZHAO [c], Song LUO [c] and Zhi GUAN [a,d,1]

[a] *Key Laboratory of High Confidence Software Technologies (Peking University), MoE, Beijing, China*

[b] *Department of Computer Science and Technology, EECS, Peking University, Beijing, China*

[c] *School of Computer Science and Engineering, Chongqing University of Technology, Chongqing, China*

[d] *National Engineering Research Center for Software Engineering, Peking University, Beijing, China*

Abstract. Accountable authority identity-based encryption (A-IBE) is an extension of identity-based encryption (IBE) in which private key's source can be traced, i.e., whether the key comes from a private key generator or a user. SM9 is an official cryptography standard of China which defines a practical IBE scheme. In this paper, we construct a practical A-IBE scheme from the SM9-IBE scheme. Our A-IBE scheme has public traceability and is proven secure if the based SM9-IBE scheme is secure. Compared with other A-IBE schemes, our A-IBE scheme has better efficiency in encryption and decryption.

Keywords. Accountable authority, identity-based encryption, SM9, bilinear group

1. Introduction

Identity-based encryption (IBE) [1] was proposed to simplify the public-key infrastructure. Unlike traditional public key encryption, any meaningful strings related to a user's identity, such as IP address, e-mail address, phone number or ID number, can be used to form a public key. Messages can be encrypted to any identity, but the ciphertext can only be decrypted by the owner of the target identity.

Though IBE has many appealing advantages, it has an inherent problem called key escrow. A trusted authority named as private key generator(PKG) exists in an IBE scheme which selects the system parameters, generates master keys and all users' private keys. If a private key is used for illegal purposes, it is hard to distinguish this key comes from the PKG or the user.

The key escrow problem is hard to solve until Goyal [2] introduced the concept of accountable authority IBE (A-IBE). In A-IBE schemes, to obtain his own private key,

[1] Corresponding Author: guan@pku.edu.cn

the user should run a interactive key generation protocol with the PKG. Only the user knows the generated private key. If the PKG is dishonest and generates another key for malicious usage, we can use an additional tracing algorithm to catch it and sue it in the court of law.

SM9 [3] is an official cryptography standard of China in which a set of pairing-based cryptographic schemes from pairings are defined, including identity-based encryption, digital signature, authenticated key exchange protocol and one recommended 256-bit BN curve. SM9 can be implemented in different platforms and it has better computation efficiency and shorter ciphertext than three other schemes included in ISO/IEC 18033-5 [4]. Nowadays, the International Organization for Standardization adopts the signature scheme and the encryption scheme of SM9 as ISO/IEC 14888-3:2018 [5] and ISO/IEC 18033-5 [6], respectively.

Our Contribution. In our paper, we build a new A-IBE scheme based on the SM9-IBE scheme. As a result, our A-IBE scheme conforms to the Chinese standard and the international standard since the based SM9-IBE scheme is standard. To the best of our knowledge, it is the first A-IBE scheme which is compatible with the Chinese cryptographic standard. Our A-IBE scheme has public traceability, i.e., everyone can trace the source of a decryption key with the help of a public tracing key. Furthermore, it is secure and efficient. Our A-IBE scheme is proven secure if the based SM9-IBE scheme is secure. Analysis shows that our A-IBE scheme has better efficiency in encryption and decryption than other A-IBE schemes, which is very important for current online applications.

Related Works. Goyal [2] first introduced the notion of A-IBE and he proposed a white-box A-IBE scheme and a weak black-box A-IBE scheme, respectively. Goyal et al. [7] presented the first full black-box A-IBE scheme. A weak black-box A-IBE scheme was proposed by Libert and Vergnaud [8] in which the private keys and ciphertexts have constant sizes. Lai et al. [9] proposed the first A-IBE scheme with public traceability in which the tracing key is public and anyone can trace a decryption key. Two generic constructions of A-IBE were proposed by Sahai and Seyalioglu [10], Kiayias and Tang [11] respectively. The former is full black-box secure while the latter is weak black-box secure. To achieve full and efficient black-box A-IBE, Zhao et al. [12] presented a new generic construction and gave an efficient instantiation from Park-Lee IBE scheme [13]. Recently, Zhao et al. [14] and Zhao et al. [15] extend A-IBE to accountable authority identity-based broadcast encryption and accountable authority identity-based revocable encryption, respectively.

Organization. The rest of this paper is organized as follows. Some necessary background knowledge is provided in Section 2. We first propose a modified SM9-IBE scheme in Section 3. Based on this modified SM9-IBE scheme, we then propose a new A-IBE scheme and prove its security in Section 4. Next we give a brief analysis for our A-IBE scheme in Section 5. In Section 6 the paper is concluded with future work.

2. Preliminaries

Definition 2.1. *Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two additive cyclic group and $\mathbb{G}_T$ be a multiplicative groups and they all have prime order N. Let P_1 be a generator of $\mathbb{G}_1$ while P_2 be a generator of $\mathbb{G}_2$. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear map which satisfies the following properties:*

(i) $\forall x,y \in \mathbb{Z}_N$, $e([x]P_1,[y]P_2) = e(P_2,P_2)^{xy}$ *(Bilinearity).*
(ii) $e(P_1,P_2) \neq 1$ *(Non-degeneracy).*

We assume that the bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ *and the group operation in* $\mathbb{G}_1$ *and* $\mathbb{G}_2$ *can be computed efficiently. We also assume that* $(N,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,P_1,P_2)$ *can be obtained by an efficient algorithm* $\mathscr{G}$ *which takes a system security parameter* λ *as input.*

If there exists an isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$ (or $\mathbb{G}_1$ equals to $\mathbb{G}_2$), we say that the bilinear groups are symmetric. Symmetric groups are easier to describe the construction of a scheme but have less computation efficiency than asymmetric groups.

The following four algorithms are included in an IBE scheme: the **Setup** algorithm for system setup, the **KeyGen** algorithm to generate private keys, the **Encrypt** algorithm to encrypt messages, and the **Decrypt** algorithm to decrypt ciphertext. The accountable authority IBE scheme has two extra algorithms: **Trace** algorithm is used to trace a decryption box $\mathbb{D}_{\mathsf{ID}}$ whether it is generated from the PKG or the user with the help of the public tracing token list, and **Judge** algorithm is used to judge a tracing key for some identity or not.

The CPA security or semantic security game defined for IBE schemes consists of five stages: **Setup**, **Query Phase 1, 2**, **Challenge** and **Guess**. The adversary submits a challenging identity ID^* and two equal-length messages M_1,M_2 at the **Challenge** stage and can query any identities in **Query Phase 1, 2** except the challenging identity. Finally at the **Guess** stage the adversary will be returned a ciphertext encrypted to ID^* and M_μ where $\mu \in \{0,1\}$ is random. The adversary should give a guess μ' of μ and his advantage is $|\Pr[\mu' = \mu] - \frac{1}{2}|$. An IBE scheme is semantically secure if no p.p.t adversary has non-negligible advantage in winning the above game. A-IBE has two extra security definitions called **DishonestPKG** security which is used to trace whether a decryption box(white-box or black-box) is generated by the PKG, while **DishonestUser** security is used to prove that nobody except the key owner can produce a valid decryption box.

3. A Modified SM9-IBE Scheme

We present a modified SM9-IBE scheme in this section. Compared with the original SM9-IBE scheme, we simplify the encryption and the decryption algorithm. This modified scheme has only semantic (CPA) security, while the initial SM9-IBE scheme is CCA2 secure. We use this modified scheme because in the security proof we would modify the original SM9-IBE ciphertext to a valid A-IBE ciphertext. However, this is infeasible since the original SM9-IBE scheme has an integrity check for its ciphertext.

Let $H_1()$ be a cryptographic hash function and *hid* be the identifier of the encryption private key generating function, we propose the modified SM9-IBE scheme as follows.

- **Setup**(1^λ): The algorithm gets public parameter PP $= (N,\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P_1,P_2, e)$ from $\mathscr{G}(\lambda)$. It randomly chooses an integer $ke \in [1,N-1]$, computes $P_{pub-e} = [ke]P_1$ and $\Omega = e(P_{pub-e},P_2)$. The public key is PK $= (\mathrm{PP},P_{pub-e},\Omega)$ and the master secret key MSK is ke.
- **KeyGen**(MSK, ID): The algorithm first computes $t_1 = H_1(\mathsf{ID}||hid,N)+ke$. If $t_1 = 0$, it runs the **Setup** algorithm again. Otherwise, it computes $t_2 = ke \cdot t_1^{-1}$ and $K = [t_2]P_2$. The private key for ID is $\mathrm{SK}_{\mathsf{ID}} = (K)$.

- **Encrypt**(PK, $M \in \mathbb{G}_T$, ID): The algorithm randomly chooses an integer $s \in [1, N-1]$ and computes $Q_{\mathsf{ID}} = [H_1(\mathsf{ID}||hid, N)]P_1 + P_{pub-e}$. It then computes $C_1 = [s]Q_{\mathsf{ID}}$ and $C = M \cdot \Omega^s$. The ciphertext is $\mathrm{CT}_{\mathsf{ID}} = (C, C_1)$.
- **Decrypt**($\mathrm{CT}_{\mathsf{ID}} = (C, C_1), \mathrm{SK}_{\mathsf{ID}} = (K)$): The algorithm computes $Y = e(C_1, K)$ and the message M is recovered as $C \cdot Y^{-1}$.

Theorem 3.1. *The modified SM9-IBE scheme is semantically secure.*

The proof of this theorem is similar to the proof of the original SM9-IBE scheme except using the decryption oracle [4], so the concrete proof is omitted due to space limitation.

4. Our A-IBE Scheme

4.1. Description

We propose our A-IBE scheme which has public traceability as follows:

- **Setup**(1^λ): The algorithm first gets public parameter $\mathrm{PP} = (N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P_1, P_2, e)$ from $\mathscr{G}(\lambda)$. It chooses two random integers $ke, \alpha \in [1, N-1]$, computes $P_{pub-a} = [\alpha]P_1$, $P_{pub-e} = [ke]P_1$, $P_{pub-t} = [ke \cdot \alpha]P_1$ and $\Omega = e(P_{pub-e}, P_2)$. The public key PK is $(\mathrm{PP}, P_{pub-a}, P_{pub-e}, P_{pub-t}, \Omega)$ and the master secret key MSK is (ke, α).
- **KeyGen**(MSK, ID): The PKG interacts with a user U for identify ID in the following protocol to generate key.
  - (i) U first randomly chooses $r \in [1, N-1]$. Next, U computes $R = [r]P_2$ and sends it to the PKG. It runs an interactive zero-knowledge proof of knowledge (ZK-POK) with the PKG for the discrete log of R with respect to P_2.
  - (ii) PKG checks that the validity of the ZK-POK and it will abort if the check fails. Otherwise, the PKG randomly picks two integers $t, r' \in [1, N-1]$ and sends (R', r', K', Q', S', V') to U, where

$$R' = [\alpha]R = [r \cdot \alpha]P_2, K' = \left[\frac{ke}{H_1(\mathsf{ID}||hid, N) + ke}\right]P_2 - [t \cdot \alpha]P_2,$$

$$Q' = [t \cdot \alpha]R + [r' \cdot \alpha]P_2, S' = [t]P_2, V' = [t \cdot \alpha]P_1.$$

  - (iii) U checks the validity of the following three equations:

$$e(P_{pub-t}, R) = e(P_{pub-e}, R') \tag{1}$$

$$\begin{aligned} &e([H_1(\mathsf{ID}||hid, N)]P_1 + P_{pub-e}, K') \\ &= e(P_{pub-e}, P_2) \cdot e([H_1(\mathsf{ID}||hid, N)]P_{pub-a} + P_{pub-t}, S') \end{aligned} \tag{2}$$

$$e(P_1,Q') = e(V',R)\cdot e(P_{pub-a},P_2)^{r'} \tag{3}$$

U will abort if the check fails. Otherwise, the decryption key $\mathrm{SK}_{\mathsf{ID}}$ is (r_{ID},K), where $r_{\mathsf{ID}} = r'/r$ and

$$K = K' + [r^{-1}]Q' = \left[\frac{ke}{H_1(\mathsf{ID}||hid,N)+ke} + \frac{r'}{r}\cdot\alpha\right]P_2.$$

(iv) U sends $R_{\mathsf{ID}} = e([H_1(\mathsf{ID}||hid,N)]P_{pub-a} + P_{pub-t},P_2)^{r_{\mathsf{ID}}}$ and interacts with the PKG for a zero-knowledge proof $\mathsf{ZK}\{(r_{\mathsf{ID}},K) : R_{\mathsf{ID}} = e(P_{pub-t},P_2)^{r_{\mathsf{ID}}} \wedge e([H_1(\mathsf{ID}||hid,N)]P_1 + P_{pub-e},K) = e(P_{pub-e},P_2)\cdot R_{\mathsf{ID}}\}$ with the PKG.

(v) PKG verifies the ZK proof. If the check fails, it will abort. Finally the tracing key $t_{\mathsf{ID}} = (\mathsf{ID},R_{\mathsf{ID}})$ is added to a public tracing key list $\mathscr{TK}$.

- **Encrypt**(PK,M,ID): The algorithm randomly chooses an integer $s \in [1,N-1]$ and computes $Q_{\mathsf{ID}} = [H_1(\mathsf{ID}||hid,N)]P_1 + P_{pub-e}$. It then computes $Z_1 = [s]Q_{\mathsf{ID}}$ and $C = M\cdot\Omega^s$ and $Z_2 = e([H_1(\mathsf{ID}||hid,N)]P_{pub-a} + P_{pub-t},P_2)^s$. The ciphertext $\mathrm{CT}_{\mathsf{ID}}$ is (C,Z_1,Z_2).
- **Decrypt**($\mathrm{CT}_{\mathsf{ID}} = (C,Z_1,Z_2)$, $\mathrm{SK}_{\mathsf{ID}} = (r_{\mathsf{ID}},K)$): The algorithm computes $Y = e(C_1,K)$ and the message M is recovered as $C\cdot Y^{-1}\cdot C_2^{r_{\mathsf{ID}}}$.
- **Trace**(PK, ID, $\mathscr{TK}$, $\mathbb{D}_{\mathsf{ID}}$): Let $\mathbb{D}_{\mathsf{ID}}$ be an $\varepsilon-$useful decryption box. The algorithm will abort if the tuple $(\mathsf{ID},R_{\mathsf{ID}})$ isn't in the list of public tracing keys $\mathscr{TK}$. It then runs the following steps.

  (i) Let $ctr = 0$ be a counter. The following steps are repeated for $8\lambda/\varepsilon$ times:

  - Choose two random integers $s,s' \in [1,N-1]$ and $s \neq s'$.
  - Compute $Q_{\mathsf{ID}} = [H_1(\mathsf{ID}||hid,N)]P_1 + P_{pub-e}$.
  - A random message M is randomly chosen in $\mathbb{G}_T$. Compute $Z_1 = [s]Q_{\mathsf{ID}}$, $Z_2 = e([H_1(\mathsf{ID}||hid,N)]P_{pub-a} + P_{pub-t},P_2)^{s'}$, and $C = M\cdot\Omega^s\cdot R_{\mathsf{ID}}^{(s-s')}$.
  - The ciphertext $\mathrm{CT} = (C,Z_1,Z_2)$ is put into $\mathbb{D}_{\mathsf{ID}}$. Let $\mathbb{D}_{\mathsf{ID}}$'s output be M'. If $M = M'$, $ctr = ctr + 1$.

  (ii) The output is PKG if $ctr = 0$. If $ctr \neq 0$, the output is User.
- **Judge**: Assume that U has identity ID. He interacts with a judge in the following protocol.

  (i) Let $\mathrm{SK}_{\mathsf{ID}} = (r_{\mathsf{ID}},K)$ be the user's decryption key. U first sets $R_{\mathsf{ID}} = e(P_{pub-t},P_2)^{r_{\mathsf{ID}}}$. U then sends R_{ID} and interacts with the judge for a ZK proof $\mathsf{ZK}\{(r_{\mathsf{ID}},K) : R_{\mathsf{ID}} = e(P_{pub-t},P_2)^{r_{\mathsf{ID}}} \wedge e([H_1(\mathsf{ID}||hid,N)]P_1 + P_{pub-e},K) = e(P_{pub-e},P_2)\cdot R_{\mathsf{ID}}$.

  (ii) The judge verifies the ZK proof. If the check fails, he will abort. Finally $t_{\mathsf{ID}} = (\mathsf{ID},R_{\mathsf{ID}})$ is accepted as U's public tracing key by the judge.

Correctness.

$$e(C_1,K)^{-1} = e([s\cdot(H_1(\mathsf{ID}||hid,N)+ke)]P_1,[\frac{ke}{H_1(\mathsf{ID}||hid,N)+ke} + r_{\mathsf{ID}}\cdot\alpha]P_2)^{-1}$$

$$= e(P_1,P_2)^{-s\cdot ke - s\cdot r_{\mathsf{ID}}\cdot(H_1(\mathsf{ID}||hid,N)+ke)\cdot\alpha}$$

$$C_2^{r_{\mathsf{ID}}} = e(P_1,P_2)^{s\cdot r_{\mathsf{ID}}\cdot(H_1(\mathsf{ID}||hid,N)+ke)\cdot\alpha}$$

$$C\cdot e(C_1,K)^{-1}\cdot C_2^{r_{\mathsf{ID}}} = M\cdot e(P_1,P_2)^{s\cdot ke}\cdot e(P_1,P_2)^{-s\cdot ke} = M.$$

4.2. Security

Theorem 4.1. *If the modified SM9-IBE scheme is semantically secure, then our A-IBE scheme is also semantically secure.*

Proof. We will show that we can construct algorithm $\mathscr{B}$ which breaks the modified SM9-IBE scheme based on an adversary $\mathscr{A}$ which can break our A-IBE scheme. $\mathscr{B}$ is constructed as follows.

Setup. At first the challenger $\mathscr{C}$ outputs the public key of the modified SM9-IBE scheme $\mathrm{PK}' = \{\mathrm{PP}, P_{pub-e}, \Omega = e(P_{pub-e}, P_2)\}$ and sends it to $\mathscr{B}$. $\mathscr{B}$ randomly chooses an integer $\alpha \in [N-1]$, computes $P_{pub-t} = (P_{pub-e})^{\alpha}$, $P_{pub-a} = [\alpha]P_1$. The new public key PK is $\{e, P_1, P_2, P_{pub-a}, P_{pub-e}, P_{pub-t}, \Omega\}$ and $\{\alpha\}$ is kept secret. ThenPK is published to $\mathscr{A}$. Note that the master key of the original SM9-IBE scheme is unknown to $\mathscr{B}$.

Query Phase 1. An identity ID is submitted by $\mathscr{A}$. $\mathscr{C}$ returns $\mathscr{B}$ the private key for ID $\mathrm{SK}'_{\mathsf{ID}} = (K_0)$. Then $\mathscr{B}$ interacts with $\mathscr{A}$ in the following protocol.

(i) $\mathscr{A}$ first randomly chooses $r \in [1, N-1]$ and computes $R = [r]P_2$. It then sends R and interacts with $\mathscr{B}$ for a ZK-POK of the discrete log of R in respect of P_2.

(ii) $\mathscr{B}$ verifies the ZK-POK. It will aborts if the check fails. $\mathscr{B}$ randomly chooses two integers $t, r' \in [1, N-1]$ and sends (R', r', K', Q', S', V') to U, where $R' = [\alpha]R$, $K' = K_0 - [t \cdot \alpha]P_2$, $Q' = [t \cdot \alpha]R + [r' \cdot \alpha]P_2$, $S' = [t]P_2$ and $V' = [t \cdot \alpha]P_1$.

(iii) $\mathscr{A}$ checks whether Equations 1, 2 and 3 hold or not. $\mathscr{A}$ will abort if the check fails. $\mathscr{A}$ sets $\mathrm{SK}_{\mathsf{ID}} = (r_{\mathsf{ID}}, K)$, where $r_{\mathsf{ID}} = r'/r$ and $K = K' + [r^{-1}]Q'$.

(iv) $\mathscr{A}$ sends $R_{\mathsf{ID}} = e([H_1(\mathsf{ID}||hid, N)]P_{pub-a} + P_{pub-t}, P_2)^{r_{\mathsf{ID}}}$ to $\mathscr{B}$ and interacts with $\mathscr{B}$ for a ZK proof $\mathsf{ZK}\{(r_{\mathsf{ID}}, K) : R_{\mathsf{ID}} = e(P_{pub-t}, P_2)^{r_{\mathsf{ID}}} \wedge e([H_1(\mathsf{ID}||hid, N)]P_1 + P_{pub-e}, K) = e(P_{pub-e}, P_2) \cdot R_{\mathsf{ID}}\}$.

(v) $\mathscr{B}$ verifies the ZK proof. If the check fails, he will abort. Finally $t_{\mathsf{ID}} = (\mathsf{ID}, R_{\mathsf{ID}})$ for the identify ID is added to the public tracing key list $\mathscr{T}\mathscr{K}$.

Challenge. Let ID^* be a challenging identity and M_0, M_1 be two equal-length messages submitted by $\mathscr{A}$. $\mathscr{B}$ forwards ID^* and M_0, M_1 to $\mathscr{C}$ and is returned $\mathrm{CT}' = (C, Z_1)$ for some message $M_\mu (\mu \in \{0, 1\})$. It computes $Z_2 = e(Z_1, [\alpha]P_2)$.

Query Phase 2. $\mathscr{A}$ can query like in **Query Phase 1** except ID^*.

Guess. $\mathscr{B}$ outputs the guess μ' based on $\mathscr{A}$'s guess μ' of μ.

From above we can find that the advantage of $\mathscr{A}$ equals to $\mathscr{B}$, so if the advantage for $\mathscr{A}$ to break our A-IBE scheme is non-negligible, the advantage for $\mathscr{B}$ to break the modified SM9-IBE scheme is non-negligible. Hence, according to Theorem 3.1, this theorem is established. □

The following modified DDH-2 assumption is used to prove the **DishonestPKG** security of our A-IBE scheme.

Definition 4.1. *Let a,b are two random integers in $[1,N-1]$ and Z be randomly chosen in $\mathbb{G}_T$. Let $\overrightarrow{D} = \{[a]P_2, [1/a]P_2, e(P_1,P_2)^b\}$. For an algorithm $\mathscr{A}$, we define its advantage to break the modified DDH-2 assumption to be*

$$\left|\Pr[\mathscr{A}(\overrightarrow{D}, e(P_1,P_2)^{b/a}) = 1] - \Pr[\mathscr{A}(\overrightarrow{D}, Z) = 1]\right|.$$

For any p.p.t algorithm, if its advantage to break the modified DDH-2 assumption is non-negligible, we say that the modified DDH-2 assumption holds.

Theorem 4.2. *Under the modified DDH-2 assumption, our A-IBE scheme is* ***DishonestPKG*** *secure.*

Proof. Assume that the adversary $\mathscr{A}$ can break the **DishonestPKG** security of our A-IBE scheme. This means $\mathscr{A}$ can produce a valid decryption box $\mathbb{D}_{\mathsf{ID}}$ with **Trace**$(\mathrm{PK}, \mathsf{ID}, \mathscr{TK}, \mathbb{D}_{\mathsf{ID}}) = \mathsf{User}$. We can construct a new algorithm $\mathscr{B}$ based on $\mathscr{A}$ to break the modified DDH-2 assumption.

$\mathscr{B}$ receives an instance of the modified DDH-2 assumption $([a]P_2,\ [1/a]P_2,\ e(P_1,P_2)^b,\ T)$ and tries to decide whether $T = e(P_1,P_2)^{b/a}$ or not. $\mathscr{A}$ interacts with $\mathscr{B}$ as follows.

Setup. The public key $\mathrm{PK} = (\mathrm{PP}, P_{pub-a}, P_{pub-e}, P_{pub-t}, \Omega)$ and a challenge identity ID^* is sent from $\mathscr{A}$ to $\mathscr{B}$.

Key Generation. The key for ID^* is generated between $\mathscr{B}$ and $\mathscr{A}$ from the following steps. First it computes $R = [a]P_2$ and sends it to $\mathscr{A}$. Then $\mathscr{B}$ plays a ZK-PoK proof with $\mathscr{A}$ for the discrete log of R in respect of P_2. Though $\mathscr{B}$ doesn't know a, he can simulate the right ZK-PoK proof. Then, $\mathscr{B}$ receives (R', r', K', Q', S', V') from $\mathscr{A}$. $\mathscr{B}$ checks whether Equations 1, 2 and 3 hold or not. If no, $\mathscr{B}$ aborts. The decryption key $\mathrm{SK}_{\mathsf{ID}} = (r_{\mathsf{ID}^*}, K)$ for ID^* is set as $(r'/a, \left[\frac{ke}{H_1(\mathsf{ID}^*||hid,N)+ke} + \frac{r'}{a}\cdot\alpha\right]P_2)$ (but unknown to $\mathscr{B}$).
Next $\mathscr{B}$ sends $R_{\mathsf{ID}^*} = e([H_1(\mathsf{ID}||hid,N)]P_{pub-a} + P_{pub-t}, [1/a]P_2)^{r'}$ to $\mathscr{A}$ and gives a ZK proof for (r_{ID^*}, K). Equally, $\mathscr{B}$ can simulate the right ZK proof without knowing (r_{ID^*}, K). At last, the tracing key $t_{\mathsf{ID}^*} = (\mathsf{ID}^*, R_{\mathsf{ID}^*})$ is added to the public tracing key list $\mathscr{TK}$.

Output. At this stage, $\mathscr{A}$ outputs a decryption box $\mathbb{D}_{\mathsf{ID}^*}$ for ID^*. $\mathscr{B}$ runs the following steps in the tracing stage.

(i) Randomly choose n messages $M_1, \cdots, M_n \in \mathbb{G}_T$. For $i \in \{1,2,\cdots,n\}$, the i-th ciphertext is computed as $\mathrm{CT}^{(i)} = (C^{(i)}, Z_1^{(i)}, Z_2^{(i)})$ as

$$C^{(i)} = M \cdot \Omega^{s_i} \cdot R_{\mathsf{ID}^*}^{(s_i - s_i')} \cdot T^{-r'\cdot\delta_i}, C_1^{(i)} = [s_i]Q,$$

$$C_2^{(i)} = e([H_1(\mathsf{ID}||hid,N)]P_{pub-a} + P_{pub-t}, P_2)^{s'} \cdot e(P_1,P_2)^{b\cdot\delta_i}$$

where $Q = [H_1(\mathsf{ID}^*||hid,N)]P_1 + P_{pub-e}$ and δ_i, s_i, s_i' are chosen from $[1,N-1]$ randomly.

(ii) Set a counter $ctr = 0$. Feed $\mathbb{D}_{\mathsf{ID}^*}$ with n ciphertexts $\mathrm{CT}^{(1)}, \cdots, \mathrm{CT}^{(n)}$ and get decrypted messages $M_1', \cdots, M_n'$.

(iii) Set $ctr = ctr + 1$ for every $i = 1$ to n where $M_i = M_i'$.

Analysis. If $T = e(P_1, P_2)^{b/a}$, every $\mathrm{CT}^{(i)}$ is an ill-formed ciphertext but can be decrypted by $\mathbb{D}_{\mathsf{ID}^*}$. Hence, if the decryption box $\mathbb{D}_{\mathsf{ID}^*}$ is valid, we will get $ctr > 0$ if $T = e(P_1, P_2)^{b/a}$ or $ctr = 0$ if T is random. As a result, the modified DDH-2 assumption is broken.

□

Theorem 4.3. *If the SM9-IBE scheme has semantic security, our A-IBE scheme has* ***DishonestUser*** *security.*

Proof. The proof follows the proof of Theorem 4.1. Assume that our A-IBE scheme isn't **DishonestUser** secure. Then there is an adversary $\mathscr{A}$ can output a decryption box for an identity ID. , Hence we can use $\mathscr{A}$ to produce a decryption box for ID^*. Therefore, this decryption box can be used to decrypt the returned ciphertext and get a message M_μ. As a result, the modified SM9-IBE scheme is broken. □

5. Analysis

We now analyze our A-IBE scheme from theoretical perspective and experimental perspective. We give comparisons with other recent A-IBE schemes in the following tables. In Table 1 we compare the public key size($|\mathbf{PK}|$), the private key size($|\mathbf{SK}|$) and the ciphertext size($|\mathbf{CT}|$). In Table 2 we compare the time of encryption($\mathbf{Time}_{\mathrm{enc}}$) and the time of decryption($\mathbf{Time}_{\mathrm{dec}}$), respectively. Experiment was run on a computer with Intel Core i5-8250U 1.60GHz, 8G RAM and Ubuntu 16.04. Analysis shows our A-IBE scheme is more desirable in practice. First our scheme is compact in key size and ciphertext size. Second our scheme has shorter running time in encryption and decryption. Note that operations in asymmetric bilinear groups are more efficient than symmetric groups. Therefore, though the storage requirement of our scheme is the same as Lai et al.'s A-IBE scheme, our scheme is more efficient in encryption and decryption.

Table 1. Storage Comparison

Scheme	**Group**	$\lvert\mathbf{PK}\rvert$	$\lvert\mathbf{SK}\rvert$	$\lvert\mathbf{CT}\rvert$
Sahai et al.[2011]	Symmetric	$(2m+2)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$2n\lvert\mathbb{G}\rvert + n\lvert\mathbb{Z}_m\rvert$	$2n\lvert\mathbb{G}\rvert + n\lvert\mathbb{Z}_m\rvert + \lvert\mathbb{G}_T\rvert$
Lai et al.[2013]	Symmetric	$3\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$3\lvert\mathbb{G}\rvert + \lvert\mathbb{Z}_N\rvert$	$2\lvert\mathbb{G}\rvert + \lvert\mathbb{Z}_m\rvert + \lvert\mathbb{G}_T\rvert$
Zhao et al.[2019]	Symmetric	$3\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathbb{G}\rvert + \lvert\mathbb{Z}_N\rvert$	$2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$
Our scheme	Asymmetric	$3\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathbb{G}_2\rvert + \lvert\mathbb{Z}_N\rvert$	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$

Note: we omit the common public parameters in public key. $m = |\mathsf{ID}|$ and n is a constant fraction of m. $|\cdot|$ means the element size of $\cdot$.

6. Conclusion

We propose a new A-IBE scheme based on a modified SM9-IBE scheme in this paper. Our A-AIBE scheme has public traceability and is proven secure the based modified

Table 2. Computation Comparison(ms)

Scheme	**Time**$_{\text{enc}}$	**Time**$_{\text{dec}}$
Sahai et al.[2011]	359	2,276
Lai et al.[2013]	47	35
Zhao et al.[2019]	51	113
Our scheme	28	19

SM9-IBE scheme is secure. Experiments show that our A-IBE scheme has better efficiency in encryption and decryption than other A-IBE schemes. However, our scheme has only CPA security and weak black-box **DishonestPKG** security. We leave it an open problem to find a new A-IBE scheme based on the full SM9-IBE scheme with public traceability and other security properties.

Acknowledgements

This work is supported by the National Key Research and Development Program of China NO.2018YFB0803601.

References

[1] Adi Shamir. Identity-based cryptosystems and signatures schemes. In *Advances in Cryptology - Crypto 1984*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1984.

[2] Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 430–447. Springer, 2007.

[3] GM/T 0044-2016. Sm9 identity-based cryptographic algorithms, 2016. `http://www.gmbz.org.cn/main/postDetail.html?id=20180322410400`.

[4] Zhaohui Cheng. The sm9 cryptographic schemes. Cryptology ePrint Archive, Report 2017/117, 2017. `https://ia.cr/2017/117`.

[5] ISO/IEC. It security techniques - digital signatures with appendix - part 3: Discrete logarithm based mechanisms. Geneva, Switzerland, 2018. ISO/IEC14888-3:2018.

[6] ISO/IEC. Information technology - security techniques encryption algorithms - part 5: Identity-based ciphers; amendment 1: Sm9 mechanism. Geneva, Switzerland, 2021. ISO/IEC 18033-5.

[7] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, CCS '08, pages 427–436, New York, NY, USA, 2008. ACM.

[8] Benoît Libert and Damien Vergnaud. Towards black-box accountable authority IBE with short ciphertexts and private keys. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, volume 5443 of *Lecture Notes in Computer Science*, pages 235–255. Springer, 2009.

[9] Junzuo Lai, Robert H. Deng, Yunlei Zhao, and Jian Weng. Accountable authority identity-based encryption with public traceability. In Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings*, volume 7779 of *LNCS*, pages 326–342. Springer, 2013.

[10] Amit Sahai and Hakan Seyalioglu. Fully secure accountable-authority identity-based encryption. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*, pages 296–316. Springer, 2011.

[11] Aggelos Kiayias and Qiang Tang. Making any identity-based encryption accountable, efficiently. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 326–346. Springer, 2015.

[12] Zhen Zhao, Jianchang Lai, Willy Susilo, Baocang Wang, Yupu Hu, and Fuchun Guo. Efficient construction for full black-box accountable authority identity-based encryption. *IEEE Access*, 7:25936–25947, 2019.

[13] Jong Hwan Park and Dong Hoon Lee. An efficient IBE scheme with tight security reduction in the random oracle model. *Des. Codes Cryptogr.*, 79(1):63–85, 2016.

[14] Zhen Zhao, Fuchun Guo, Jianchang Lai, Willy Susilo, Baocang Wang, and Yupu Hu. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. *Theor. Comput. Sci.*, 809:73–87, 2020.

[15] Zhen Zhao, Ge Wu, Fuchun Guo, Willy Susilo, Yi Mu, Baocang Wang, and Yupu Hu. Black-box accountable authority identity-based revocation system. *Comput. J.*, 63(4):525–535, 2020.