2019

Efficient Construction for Full Black-Box Accountable Authority Identity-Based Encryption

Zhen Zhao
University of Wollongong, Xidian University

Jianchang Lai
Nanjing Normal University, jl967@uowmail.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Baocang Wang
Xidian University, baocang@uow.edu.au

Yupu Hu
Xidian University

See next page for additional authors

Efficient Construction for Full Black-Box Accountable Authority Identity-Based Encryption

Abstract

Accountable authority identity-based encryption (A-IBE), as an attractive way to guarantee the user privacy security, enables a malicious private key generator (PKG) to be traced if it generates and re-distributes a user private key. Particularly, an A-IBE scheme achieves full black-box security if it can further trace a decoder box and is secure against a malicious PKG who can access the user decryption results. In PKC'11, Sahai and Seyalioglu presented a generic construction for full black-box A-IBE from a primitive called dummy identity-based encryption, which is a hybrid between IBE and attribute-based encryption (ABE). However, as the complexity of ABE, their construction is inefficient and the size of private keys and ciphertexts in their instantiation is linear in the length of user identity. In this paper, we present a new efficient generic construction for full black-box A-IBE from a new primitive called token-based identity-based encryption (TB-IBE), without using ABE. We first formalize the definition and security model for TB-IBE. Subsequently, we show that a TB-IBE scheme satisfying some properties can be converted to a full black-box A-IBE scheme, which is as efficient as the underlying TB-IBE scheme in terms of computational complexity and parameter sizes. Finally, we give an instantiation with the computational complexity as O(1) and the constant size master key pair, private keys, and ciphertexts.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Zhao, Z., Lai, J., Susilo, W., Wang, B., Hu, Y. & Guo, F. (2019). Efficient Construction for Full Black-Box Accountable Authority Identity-Based Encryption. IEEE Access, 7 25936-25947.

Authors

Zhen Zhao, Jianchang Lai, Willy Susilo, Baocang Wang, Yupu Hu, and Fuchun Guo

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 3, 2019, accepted February 9, 2019, date of publication February 18, 2019, date of current version March 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2900065

Efficient Construction for Full Black-Box Accountable Authority Identity-Based Encryption

ZHEN ZHAO[1,2], JIANCHANG LAI[3], WILLY SUSILO[2], (Senior Member, IEEE), BAOCANG WANG[1], YUPU HU[1], AND FUCHUN GUO[2]

[1]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
[2]School of Computing and Information Technology, Institute of Cybersecurity and Cryptology, University of Wollongong, Wollongong, NSW 2522, Australia
[3]School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, China

Corresponding authors: Jianchang Lai (laijianchangchn@gmail.com) and Baocang Wang (bcwang79@aliyun.com)

This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802000, in part by the National Natural Science Foundation of China under Grant 61572390 and Grant U1736111, in part by the National Cryptography Development Fund under Grant MMJJ20180111, in part by the Plan For Scientific Innovation Talent of Henan Province under Grant 184100510012, and in part by the Program for Science and Technology Innovation Talents in the Universities of Henan Province under Grant 18HASTIT022.

ABSTRACT Accountable authority identity-based encryption (A-IBE), as an attractive way to guarantee the user privacy security, enables a malicious private key generator (PKG) to be traced if it generates and re-distributes a user private key. Particularly, an A-IBE scheme achieves full black-box security if it can further trace a decoder box and is secure against a malicious PKG who can access the user decryption results. In PKC'11, Sahai and Seyalioglu presented a generic construction for full black-box A-IBE from a primitive called dummy identity-based encryption, which is a hybrid between IBE and attribute-based encryption (ABE). However, as the complexity of ABE, their construction is inefficient and the size of private keys and ciphertexts in their instantiation is linear in the length of user identity. In this paper, we present a new efficient generic construction for full black-box A-IBE from a new primitive called token-based identity-based encryption (TB-IBE), without using ABE. We first formalize the definition and security model for TB-IBE. Subsequently, we show that a TB-IBE scheme satisfying some properties can be converted to a full black-box A-IBE scheme, which is as efficient as the underlying TB-IBE scheme in terms of computational complexity and parameter sizes. Finally, we give an instantiation with the computational complexity as $O(1)$ and the constant size master key pair, private keys, and ciphertexts.

INDEX TERMS Accountable authority, full black-box security, identity-based encryption.

I. INTRODUCTION

Identity-based encryption (IBE), as an attractive primitive which eliminates the necessity of certificate management in the public key infrastructure, has drawn a lot of attention. In an IBE scheme, the user public key is its identity and the corresponding private key is generated by the private key generator (PKG) using the user identity. A sender can send an encrypted message to any receiver at any time and it only needs to pre-know the identity of the receiver. This property enables IBE useful in many practical applications, such as email systems and intranets.

However, IBE suffers from an inherent problem, namely the key escrow problem. Since the PKG has full control over the user private key, it can engage in many malicious activities without taking the risk of being caught, such as decrypting any ciphertext or even generating and selling the user private key. To illustrate it clear, we consider the following scenario. Suppose Alice holds the only private key which can be used to access a $100,000 worth of database belonging to Bob's company. At a later point in time, Bob finds that a private key for the database is up for sale. To protect the company's benefit, Bob then takes Alice to court and demands compensation for potential economic loss. In such a case, Alice will pay a huge indemnity if she cannot prove her innocence to the court.

To restrict the malicious activities of the PKG, Goyal [1] proposed the concept of accountable authority identity-based encryption (A-IBE), a variant of IBE which is equipped with traceability functionality. In an A-IBE scheme, an additional

The associate editor coordinating the review of this manuscript and approving it for publication was Weizhi Meng.

tracing algorithm is used for judging whether the PKG or a suspected user who leaks a given private key. With A-IBE system, Alice in the above case can show her innocence by providing valid and convincing evidence that the private key is generated by the PKG. Furthermore, a secure A-IBE scheme should satisfy three requirements as follows.

- It protects the message confidentiality.
- A dishonest PKG is unable to frame any user. That is, the PKG cannot generate a private key which lets the user be mistakenly identified as the creator.
- A dishonest user is unable to frame the PKG. That is, the user cannot generate a private key which lets the PKG be mistakenly identified as the creator.

A-IBE can be classified into *white-box A-IBE* and *black-box A-IBE*. The white-box A-IBE can only trace the creator of a private key, whereas the black-box A-IBE is able to trace the creator of a decoder box, where a decoder box for a user can decrypt the message encrypted to the user with an unknown algorithm and unknown private key. In particular, the black-box A-IBE can be classified into *weak black-box A-IBE* and *full black-box A-IBE*, where the latter one is further secure against the dishonest PKG who can access the user decryption results. Note that the full black-box security is the strongest security model among the following three models, i.e., white-box security, weak black-box security, and full black-box security.

The first full black-box A-IBE scheme was proposed by Goyal *et al.* [2] in CCS 2008, which is a concrete construction and is selective-ID secure against dishonest users. In PKC 2011, based on [2], Sahai and Seyalioglu [3] presented a generic construction of full black-box A-IBE from a primitive called dummy identity-based encryption (D-IBE), which is a hybrid between IBE and attribute-based encryption (ABE). The instantiation of their generic construction achieves adaptive-ID dishonest user security. Without loss of generality, in the following discussion, we refer A-IBE to full black-box A-IBE unless specified otherwise.

Nevertheless, both of the proposed A-IBE schemes, [2], [3], utilize ABE. As ABE is more complex than IBE in the construction, we have that the existing A-IBE schemes are less efficient than the IBE counterpart. For example, the size of private keys and ciphertexts in both schemes are at least linear in the length of the user identity, whereas that is constant in IBE. Goyal *et al.* [2] even left an open problem for constructing an A-IBE scheme with the constant size of private keys and ciphertexts. So far, it remains unknown how to construct an A-IBE (with full black box security) system which is efficient as IBE schemes.

A. OUR CONTRIBUTIONS

Our contributions are three-fold and summarized as follows.

- We introduce a new primitive called token-based identity-based encryption (TB-IBE), which is a variant of IBE.
- Based on TB-IBE, we give a generic construction of full black-box accountable identity-based encryption (A-IBE) which is as efficient as the underlying TB-IBE in terms of parameter sizes and computational complexity.
- Finally, we give an instantiation of our generic construction based on Park-Lee IBE scheme [4], where the instantiation achieves adaptive-ID dishonest user security.

In a TB-IBE scheme, both the private key and the ciphertext consist of an additional element called token. A user with identity ID_k can use its private key d_{ID} which is comprised of a token t_k to decrypt a ciphertext that is encrypted to ID_c and consists of a token t_c if and only if $ID_k = ID_c$ and $t_k \neq t_c$. In the security model of traditional IBE, the adversary is not allowed to query the private key of identity ID^* to be challenged. In contrast, in the security model of TB-IBE, the adversary can query the private key of ID^* with the restriction that the returned private key d_{ID^*} has the same token as the generated challenge ciphertext for ID^*.

Then, we show that any TB-IBE scheme satisfying three defined properties, namely Key-Well-Form, Cip-Well-Form, and KG-Transfer, can be converted to a full black-box A-IBE scheme following the generic construction. For an identity in the converted A-IBE scheme, given any possible private key (associated with a token t_k), there exist a negligible fraction of valid ciphertexts (associated with a token t_c) that cannot be decrypted by this key ($t_k = t_c$). This is used for tracing in the converted A-IBE scheme. Given a user private key d_{ID} and a decoder box $\mathbb{D}$, the creator of $\mathbb{D}$ can be traced by feeding it with those ciphertexts which cannot be decrypted using d_{ID}. If $\mathbb{D}$ returns the correct message, it is believed that the PKG creates $\mathbb{D}$. On the other hand, this is not helpful for the malicious PKG who is allowed to access decryption queries, since the PKG can only find such a ciphertext with a negligible probability.

To construct a full black-box A-IBE scheme based on Park-Lee IBE scheme, we first show that Park-Lee IBE scheme is a TB-IBE scheme and it is secure with a random oracle under the defined security model for TB-IBE. Then, we demonstrate that Park-Lee IBE scheme satisfies the required three properties such that it can be transferred to a full black-box A-IBE scheme following our generic construction. To show the efficiency of our instantiation, we present the comparison with other existing full black-box A-IBE schemes [2], [3] and the fundamental Park-Lee IBE scheme [4] in Table. 1. As shown in Table. 1, the master public/secret key pair, private keys, and ciphertexts in our scheme consist of the same constant number of group elements as Park-Lee IBE scheme, whereas most of these parameters are at least linear in the length of identity in [2] and [3]. Besides this, the computation cost of encryption and decryption of our construction is also constant, i.e., the computational complexity is $O(1)$, which is comparable to Park-Lee IBE scheme and more efficient than that of [2] and [3].

TABLE 1. Comparison of parameter sizes and computation cost.

	A-IBE scheme [2]	A-IBE scheme [3]	Our A-IBE scheme	Park-Lee IBE scheme [4]
$\|mpk\|$	$(2l+nm+1)\|\mathbb{G}\|$	$(2l+2)\|\mathbb{G}\|$	$2\|\mathbb{G}\|$	$2\|\mathbb{G}\|$
$\|msk\|$	$(2l+nm+1)\|\mathbb{Z}_p\|$	$\|\mathbb{G}\|$	$\|\mathbb{Z}_p\|$	$\|\mathbb{Z}_p\|$
$\|d_{ID}\|$	$(l+km)\|\mathbb{G}\|+km\|\mathbb{Z}_n\|$	$2t\|\mathbb{G}\|+t\|\mathbb{Z}_l\|$	$3\|\mathbb{G}\|+\|\mathbb{Z}_p\|$	$3\|\mathbb{G}\|+\|\mathbb{Z}_p\|$
$\|CT\|$	$(l+km)\|\mathbb{G}\|+km\|\mathbb{Z}_n\|+\|\mathbb{G}_T\|$	$2t\|\mathbb{G}\|+t\|\mathbb{Z}_l\|+\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+\|\mathbb{Z}_p\|+\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+\|\mathbb{Z}_p\|+\|\mathbb{G}_T\|$
Encryption	$(l+km+1)\mathcal{E}$	$\mathcal{P}+(2t+1)\mathcal{E}$	$\mathcal{P}+4\mathcal{E}$	$\mathcal{P}+4\mathcal{E}$
Decryption	$(3l+2km+m\tau)\mathcal{P}+m\tau\mathcal{E}$	$(2t+2\tau+1)\mathcal{P}+((t-\tau)\tau+\tau+1)\mathcal{E}$	$6\mathcal{P}+2\mathcal{E}$	$3\mathcal{P}+\mathcal{E}$

$l=|ID|$. $n=\lambda$. $m=\log^2(n)$. $|\mathbb{G}|$: the size of an element in the multiplicative cyclic group $\mathbb{G}$ of prime order p. $|\mathbb{G}_T|$: the size of an element in the multiplicative cyclic group $\mathbb{G}_T$ of prime order p. $|\mathbb{Z}_p|$: the size of an element in the additive group $\mathbb{Z}_p$. k: a constant fraction of n. t: a constant fraction of l. τ: the size of a threshold. $\mathcal{P}$: pairing. $\mathcal{E}$: exponentiation in group $\mathbb{G}$.

B. RELATED WORK

The notion of Accountable Authority Identity-Based Encryption (A-IBE) was first introduced by Goyal in [1], where the two proposed schemes achieve white-box security and weak black-box security, respectively. Later, Goyal *et al.* [2] proposed the first full black-box A-IBE scheme with security against dishonest users in the selective model. Libert and Vergnaud [5] proposed a weak black-box A-IBE scheme with the constant size of private keys and ciphertexts. A generic construction of A-IBE with full black-box security was presented by Sahai and Seyalioglu in [3], using a primitive called dummy IBE. They enhanced Goyal *et al.*s' scheme [2] and put forward the first adaptive-ID secure A-IBE scheme in the full black-box model. Kiayias and Tang [6] presented a generic construction, showing how to transfer any IBE scheme to a weak black-box A-IBE scheme.

A-IBE with additional functionalities was studied in [6]–[8]. Au *et al.* [7] extended the white-box A-IBE scheme with retrievability, which means the master secret key of the PKG can be retrieved if more than one private key for a user is created. The public traceability of A-IBE was considered in [8] where the tracing can be performed with a public key. The authors gave a weak black-box A-IBE scheme with public traceability. The generic construction presented in [6] was extended to support identity reuse.

Accountability in attribute-based encryption (ABE) was introduced in [9] including accountable authority and a new feature called user accountability. ABE with user accountability enables tracing a given private key or decoder box to its creator among numerous suspected users, where the authority is assumed to be fully trusted. Whereas in accountable authority ABE, it is necessary to further distinguish the PKG from the user as the creator since the authority is assumed to be semi-trusted. ABE schemes supporting user accountability were studied in [10]–[13]. ABE schemes with user accountable authority and user accountability were given in [14]–[16], where [14] and [15] consider the white-box security and [16] considers the black-box security. However, the black-box security in A-ABE only refers to the weak black-box security in A-IBE.

The defined notion of *token-based identity-based encryption* can be traced back to the dual system encryption for IBE introduced by Waters in [17], where both the private key and the ciphertext contain a *tag*, and one ciphertext cannot be decrypted by a private key if their tags are identical. The tags were created in order to obtain the adaptive security. We note that the dual system encryption with tags cannot be applied as a building block for our generic construction since we cannot check whether the ciphertext is well-formed or not. IBE schemes with tags were also studied in [4], [18], and [19] for adaptive security.

C. ORGANIZATION

The rest of this paper is organized as follows. In Section II, we recall the definitions and security models of full black-box A-IBE schemes. In Section III, we propose an efficient generic construction of full black-box A-IBE scheme along with its security proof based on a new primitive, namely token-based identity-based encryption. In Section IV, we describe a concrete scheme of our generic construction. Finally, we conclude this paper in Section V.

II. FULL BLACK-BOX ACCOUNTABLE AUTHORITY IBE

In this section, we review the formal definitions and security models for full black-box accountable authority identity-based encryption (A-IBE).

A. DEFINITIONS

An A-IBE scheme is a variant of IBE and it is able to distinguish the PKG from the user as the creator of a given ϵ-useful decoder box $\mathbb{D}$ for *ID* (defined in Definition 1). In traditional IBE, the user private key is completely generated by the PKG. But, in A-IBE, the private key generation process is performed by the PKG and the user together via running a key generation protocol to achieve the traceability. More precisely, an A-IBE scheme comprises five algorithms as follows.

- Setup (1^λ). Taking as input a security parameter λ, the setup algorithm outputs a master public/secret key pair (mpk, msk).
- KeyGenPro (mpk, msk, ID). This is a protocol in which a user U interacts with the PKG to obtain a private key d_{ID} for an identity *ID*.
  - *Inputs:*
    PKG takes as input (mpk, msk) and *ID*;
    U takes as input *mpk* and *ID*.
  - *Outputs:*
    U receives a private key d_{ID} as its secret output.

- Encrypt (mpk, ID, M). Taking as input mpk, ID, and a message M, the encrypt algorithm outputs a ciphertext CT for (ID, M).
- Decrypt (mpk, d_{ID}, CT). Taking as input mpk, a ciphertext CT, and a private key d_{ID} for ID, the decrypt algorithm outputs M or $\perp$.
- Trace $(mpk, d_{ID}, \mathbb{D})$. Taking as input mpk, a "well-formed" private key d_{ID} for ID,[1] and an ϵ-useful decoder box $\mathbb{D}$ for ID, the trace algorithm outputs PKG or U according to that $\mathbb{D}$ is generated by PKG or U.

Correctness. The correctness of an A-IBE scheme requires that for any $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda)$ and $d_{ID} \leftarrow \mathsf{KeyGenPro}(mpk, msk, ID)$, we have that

$$\mathsf{Decrypt}(mpk, d_{ID}, \mathsf{Encrypt}(mpk, ID, M)) = M.$$

Definition 1 (ϵ-Useful Decoder Box [3]): For non-negligible ϵ, a probabilistic polynomial time algorithm $\mathbb{D}$ is an ϵ-useful decoder box for the identity ID if:

$$\Pr[M \leftarrow \mathbb{D}(\mathsf{Encrypt}(mpk, ID, M))] \geq \epsilon.$$

B. SECURITY MODELS

A secure A-IBE scheme is required to satisfy three security requirements. First, it should capture the message confidentiality as IBE schemes. Next, it should guarantee that in the tracing algorithm, the user cannot be framed by the PKG. Then, the guarantee should also be applied to ensure that the PKG cannot be framed by the user. We define the security models of an A-IBE scheme to capture its security via the following three games, i.e., IND-ID-CPA game, Dishonest PKG game, and dishonest user game, which are played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

1) IND-ID-CPA GAME

The IND-ID-CPA security of an A-IBE scheme is similar to that in the IBE scheme except for the key generation process.

Setup. $\mathcal{C}$ runs the setup algorithm Setup to generate a master key pair (mpk, msk) and sends mpk to $\mathcal{A}$.

Phase 1. In this phase, $\mathcal{A}$ is allowed to make private key queries on adaptively chosen identities. For a queried identity ID, $\mathcal{A}$ interacts with $\mathcal{C}$ to run the key generation protocol KeyGenPro to generate the corresponding private key d_{ID}. Note that $\mathcal{A}$ will obtain the same private key for the same queried ID.

Challenge. Once $\mathcal{A}$ decides that Phase 1 is over, it submits two different messages M_0^*, M_1^* from the message space and an identity ID^* for challenge with the restriction that ID^* was not queried in Phase 1. $\mathcal{C}$ then picks a random bit $\mu \in \{0, 1\}$, runs the encrypt algorithm Encrypt to generate the challenge ciphertext CT^* with (ID^*, M_μ^*), and sends CT^* to $\mathcal{A}$.

Phase 2. In this phase, $\mathcal{A}$ is allowed to issue more private key queries on the identity ID with the restriction that $ID \neq ID^*$. $\mathcal{C}$ responds to $\mathcal{A}$ the same as Phase 1.

Guess. Finally, $\mathcal{A}$ outputs its guess μ' of μ and wins the game if $\mu' = \mu$.

The advantage of $\mathcal{A}$ in winning this game is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\text{IND-ID-CPA}}(\lambda) = \left|\Pr[\mu' = \mu] - 1/2\right|.$$

If $\mathcal{A}$ is allowed to make decryption queries on the ciphertext CT encrypted with ID in Phase 1 and Phase 2 with the restriction that $CT \neq CT^*$ if CT is generated with ID^*, then we have the IND-ID-CCA game.

2) DISHONEST PKG GAME

In the dishonest PKG security, $\mathcal{C}$ acts as an honest user and $\mathcal{A}$ acts as a malicious PKG who tries to output an ϵ-useful decoder box $\mathbb{D}^*$ for ID^* and frames U.

Setup. $\mathcal{C}$ receives the master public key mpk and a challenge identity ID^* from $\mathcal{A}$.

KeyGen. $\mathcal{C}$ interacts with $\mathcal{A}$ to run the key generation protocol KeyGenPro to generate the corresponding private key d_{ID^*} for ID^*. If neither party aborts, $\mathcal{C}$ receives d_{ID^*} as its secret output.

Query. In this phase, $\mathcal{A}$ is allowed to make decryption queries on adaptively chosen ciphertexts CT, $\mathcal{C}$ runs the decrypt algorithm Decrypt to obtain the decryption $M/\perp$ and sends it to $\mathcal{A}$.

Frame. Finally, $\mathcal{A}$ outputs an ϵ-useful decoder box $\mathbb{D}^*$ for the identity ID^* and wins the game if $\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = U$.

We define $\Pr[\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = U]$ as the advantage of $\mathcal{A}$ in winning this game.

3) DISHONEST USER GAME

In the dishonest user security, $\mathcal{C}$ acts as an honest PKG and $\mathcal{A}$ acts as a malicious user U who tries to output an ϵ-useful decoder box $\mathbb{D}^*$ for ID^* and frames PKG.

Setup. $\mathcal{C}$ runs the setup algorithm Setup to generate a master key pair (mpk, msk) and sends mpk to $\mathcal{A}$.

KeyGen. In this phase, $\mathcal{A}$ is allowed to make private key queries on adaptively chosen identities. For a queried identity ID, $\mathcal{A}$ interacts with $\mathcal{C}$ to run the key generation protocol KeyGenPro to generate the corresponding private key d_{ID}.

Frame. Finally, $\mathcal{A}$ outputs a private key d_{ID^*} for ID^* and an ϵ-useful decoder box $\mathbb{D}^*$ for ID^* and wins the game if $\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = PKG$.

We define $\Pr[\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = PKG]$ as the advantage of $\mathcal{A}$ in winning this game. If $\mathcal{A}$ is required to declare the challenge identity ID^* before the setup phase, we have the selective-ID dishonest user security.

Definition 2 (Security of A-IBE): A full black-box accountable authority identity-based encryption scheme is secure if all polynomial time adversaries have at most a negligible advantage in the **IND-ID-CPA Game**, the **Dishonest PKG Game**, and the **Dishonest User Game**.

III. GENERIC CONSTRUCTION FROM TOKEN-BASED IBE

In this section, we give a generic construction of full black-box accountable authority identity-based encryption from a

[1]The "well-formed" here means that the private key d_{ID} is a probable output of the key generation protocol KeyGenPro for ID.

new primitive called *token-based identity-based encryption (TB-IBE)*.

A. TOKEN-BASED IBE

We first formalize the definition and the security model of a new primitive, *token-based identity-based encryption (TB-IBE)*. In a TB-IBE scheme, the private key and the ciphertext contain an additional element called *token*. The private key of an identity ID can decrypt a ciphertext encrypted to ID only when their tokens are different. More precisely, a TB-IBE scheme consists of four algorithms below.

- $\mathsf{T.Setup}(1^\lambda)$. Taking as input a security parameter λ, it outputs a master public/secret key pair $(T.mpk, T.msk)$.
- $\mathsf{T.KeyGen}(T.mpk, T.msk, ID, t_k)$. Taking as input $(T.mpk, T.msk)$, an identity ID, and a token t_k, it generates the output private key $T.d_{ID}$, where $T.d_{ID}$ naturally contains t_k.
- $\mathsf{T.Encrypt}(T.mpk, ID, M, t_c)$. Taking as input $T.mpk$, an identity ID, a message M, and a token t_c, it generates the output ciphertext $T.CT$, where $T.CT$ naturally contains t_c.
- $\mathsf{T.Decrypt}(T.mpk, T.d_{ID}, T.CT)$. Taking as input $T.mpk$, a private key $T.d_{ID}$ created with (ID, t_k), and a ciphertext $T.CT$, it outputs a message M or $\perp$.

Correctness. The correctness of a TB-IBE scheme requires that for any $(T.mpk, T.msk) \leftarrow \mathsf{T.Setup}(1^\lambda)$ and $T.d_{ID} \leftarrow \mathsf{T.KeyGen}(T.mpk, T.msk, ID, t_k)$, we have that

$$\mathsf{T.Decrypt}(T.mpk, T.d_{ID}, \mathsf{T.Encrypt}(T.mpk, ID, M, t_c)) = \begin{cases} M & \text{if } t_k \neq t_c \\ \perp & \text{otherwise.} \end{cases}$$

Since not all the ciphertexts encrypted to ID can be decrypted by the private key generated for ID in a TB-IBE scheme, it is possible to generate a private key such that some known ciphertexts cannot be decrypted with it. With this property, we can generate the private key of the challenge identity in the security model with the restriction that it cannot decrypt the challenge ciphertext. Then, we define a new security model of TB-IBE to captures the indistinguishable security against chosen-plaintext attacks (IND-tID-CPA) by the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

1) IND-TID-CPA GAME

The IND-tID-CPA security of a TB-IBE scheme is defined as follows.

Setup. $\mathcal{C}$ runs the setup algorithm $\mathsf{T.Setup}$ to generate a master key pair $(T.mpk, T.msk)$ and sends $T.mpk$ to $\mathcal{A}$.

Phase 1. In this phase, $\mathcal{A}$ is allowed to make private key queries on adaptively chosen identities. For a queried identity ID, $\mathcal{C}$ randomly chooses a token t_k, runs the key generation algorithm $\mathsf{T.KeyGen}$ to generate the corresponding private key $T.d_{ID}$, and sends it to $\mathcal{A}$. For the same queried identity, $\mathcal{C}$ responds to $\mathcal{A}$ with the same private key.

Challenge. Once $\mathcal{A}$ decides that Phase 1 is over, it outputs two different messages M_0^*, M_1^* from the message space and an identity ID^* for challenge, where ID^* can be one of the queried identities in Phase 1. $\mathcal{C}$ responds as follows.

- If ID^* was not queried in Phase 1, $\mathcal{C}$ picks a random bit $\mu \in \{0, 1\}$ and a random token t_c^*, runs the encrypt algorithm $\mathsf{T.Encrypt}$ to generate the challenge ciphertext $T.CT^*$ with (ID^*, M_μ^*, t_c^*), and sends it to $\mathcal{A}$.
- Otherwise, ID^* was queried in Phase 1. Let $T.d_{ID^*}$ associate with the token t_k be the corresponding private key. $\mathcal{C}$ picks a random bit $\mu \in \{0, 1\}$, sets $t_c^* = t_k$, and runs the encrypt algorithm $\mathsf{T.Encrypt}$ to generate the challenge ciphertext $T.CT^*$ with (ID^*, M_μ^*, t_c^*). It then sends $T.CT^*$ to $\mathcal{A}$.

Phase 2. In this phase, $\mathcal{A}$ is allowed to issue more private key queries on adaptively chosen identities which can contain ID^*. For a queried identity ID, $\mathcal{C}$ responds as follows.

- If $ID = ID^*$ and ID^* was not queried before, $\mathcal{C}$ sets $t_k^* = t_c^*$, runs the key generation algorithm $\mathsf{T.KeyGen}$ to generate the corresponding private key $T.d_{ID^*}$ with (ID^*, t_k^*), and sends it to $\mathcal{A}$.
- Otherwise, $\mathcal{C}$ responds to $\mathcal{A}$ the same as Phase 1.

Guess. Finally, $\mathcal{A}$ outputs its guess μ' of μ and wins the game if $\mu' = \mu$.

The advantage of $\mathcal{A}$ in winning this game is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}tID\text{-}CPA}}(\lambda) = \left|\Pr[\mu' = \mu] - 1/2\right|.$$

It is easy to see that IND-tID-CPA security covers IND-ID-CPA security. Additionally, if $\mathcal{A}$ is allowed to make decryption queries in Phase 1 and Phase 2, we have the indistinguishable security against chosen-ciphertext attacks of a TB-IBE scheme (IND-tID-CCA).

Definition 3 (Security of TB-IBE): A token-based identity-based encryption scheme is IND-tID-CPA secure if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}tID\text{-}CPA}}(\lambda)$ is negligible.

B. GENERIC CONSTRUCTION

Then we show that a TB-IBE scheme can be converted to an A-IBE scheme if it satisfies the following three properties, i.e., Key-Well-Form, Cip-Well-Form, and Key-Transfer. Furthermore, the converted A-IBE scheme is comparable to the underlying TB-IBE scheme in terms of parameter sizes and computational complexity.

- **(Key-Well-Form)**. Let $\mathcal{KS}$ be the private key range of $\mathsf{T.KeyGen}(T.mpk, T.msk, ID, t_k)$ for a given identity ID and any token t_k. There exists a key sanity check algorithm as follows.

  $\mathsf{T.KCheck}(T.mpk, T.d_{ID})$: taking as input $T.mpk$ and a private key $T.d_{ID}$ for ID, it outputs 1 if $T.d_{ID}$ is well-formed, i.e.

  $$T.d_{ID} \in \mathcal{KS}.$$

  Otherwise, it outputs 0.

- **(Cip-Well-Form)**. Let $\mathcal{CS}$ be the ciphertext range of T.Encrypt$(T.mpk, ID, M, t_c)$ for a given identity ID, a given message M, and any token t_c. There exists a ciphertext sanity check algorithm as follows.

  T.CCheck$(T.mpk, T.CT)$: taking as input $T.mpk$ and a ciphertext $T.CT$ created with (ID, M), it outputs 1 if $T.CT$ is well-formed, i.e.

  $$T.CT \in \mathcal{CS}.$$

  Otherwise, it outputs 0.

- **(KG-Transfer)**. There exists a secure key generation protocol in which a user U with identity ID interacts with the PKG to obtain its corresponding private key.

  T.KeyGenPro$(T.mpk, T.msk, ID)$:
  - *Inputs:*
    PKG takes as input $(T.mpk, T.msk)$ and ID;
    U takes as input $T.mpk$ and ID;
  - *Outputs:*
    U receives a private key $T.d_{ID}$ created with (ID, t_k), if $1 \leftarrow$ T.KCheck$(T.mpk, T.d_{ID})$, U receives $T.d_{ID}$ as its secret output.

  Note that the token t_k is hidden in the key generation protocol such that the PKG cannot control the user private key. Furthermore, the security of the key generation protocol requires that the following KG-Replace and KG-Anonymity holds.
  - **(KG-Replace).** Replacing the key generation algorithm T.KeyGen with the key generation protocol T.KeyGenPro, the TB-IBE scheme is still IND-tID-CPA secure.
  - **(KG-Anonymity).** PKG has negligible probability in guessing the token t_k in the user private key $T.d_{ID}$.

Using the original three algorithms of TB-IBE, i.e., T.Setup, T.Encrypt, and T.Decrypt, the transferred A-IBE scheme replaces T.KeyGen with T.KeyGenPro and adds a new trace algorithm called Trace.

Generic Construction. We give a generic construction of an A-IBE scheme below.

- Setup(1^λ). Taking as the input the security parameter λ, it runs T.Setup(1^λ) to generate the master public/secret key pair $(T.mpk, T.msk)$ and sets the output master key pair as $(mpk, msk) = (T.mpk, T.msk)$.
- KenGenPro(mpk, msk, ID). For an identity ID, U interacts with the PKG to run the key generation protocol T.KeyGenPro$(T.mpk, T.msk, ID)$ and obtain a corresponding well-formed private key $T.d_{ID}$ created with t_k. U sets its private key as $d_{ID} = T.d_{ID}$.
- Encrypt(mpk, ID, M, t_c). Taking as input mpk, an identity ID, a message M, and a token t_c, it runs T.Encrypt$(T.mpk, ID, M, t_c)$ to generate a corresponding ciphertext $T.CT$ with (ID, M, t_c) and sets the output ciphertext as $CT = T.CT$.
- Decrypt(mpk, d_{ID}, CT). Taking as input mpk, a private key d_{ID} created with (ID, t_k), and a ciphertext CT, it aborts if T.CCheck$(T.mpk, T.CT)$ returns 0. Otherwise, it runs T.Decrypt$(T.mpk, T.d_{ID}, T.CT)$ to obtain the return decryption $M/\perp$ and sets the output as the return decryption.
- Trace$(mpk, d_{ID}, \mathbb{D})$. Taking as input mpk, a private key d_{ID} created with (ID, t_k), and an ϵ-useful decoder box $\mathbb{D}$ for the same identity ID, it aborts if T.KCheck $(T.mpk, T.d_{ID})$ returns 0. Otherwise, the trace algorithm performs as follows.
  a. Initialize a counter $ctr \leftarrow 0$ and repeat the next steps $L = \lambda/\epsilon$ times.
     1) Set $t_c = t_k$ and randomly choose a message M, run Encrypt(mpk, ID, M, t_c) to generate a ciphertext CT with (ID, M, t_c).
     2) Feed the decoder box $\mathbb{D}$ with CT. If $\mathbb{D}$ outputs M' such that $M' = M$, increment ctr.
  b. If $ctr = 0$, it outputs U. Otherwise, it outputs PKG.

In the trace algorithm, the private key d_{ID} created with the token t_k cannot decrypt the ciphertext CT created with the token t_c since $t_k = t_c$. Then, if $\mathbb{D}$ is generated with the input private key d_{ID}, it cannot correctly decrypt the ciphertext CT. Let the message space be $\mathcal{M}$ whose size is exponential in the size of security parameter, the probability that $\mathbb{D}$ correctly guesses the message is $1/|\mathcal{M}|$ which is negligible. Then, if $\mathbb{D}$ can decrypt the ciphertext correctly, PKG is suspected to be the creator of $\mathbb{D}$.

More specifically, from the generic construction, the converted A-IBE scheme has the same master key pair, private keys, and ciphertexts as the underlying TB-IBE scheme. Furthermore, the encryption process of the converted A-IBE scheme is just the same as the underlying TB-IBE scheme while the decryption process adds an additional ciphertext sanity check which costs constant operations (since the ciphertext size is constant). This leads to an A-IBE scheme which is as efficient as the TB-IBE scheme in terms of parameter sizes (master key pair, private keys, and ciphertexts) and computational complexity (encryption and decryption).

C. SECURITY ANALYSIS

Finally, we give the security analysis of our generic construction.

Theorem 1: The constructed A-IBE scheme is secure when the underlying TB-IBE scheme satisfies the three properties, i.e. Key-Well-Form, Cip-Well-Form, and KG-Transfer.

Proof: According to Definition 2, an A-IBE scheme is secure if the advantages of an adversary in winning the IND-ID-CPA game, dishonest PKG game, and dishonest user game are all negligible. We give the proof for these three securities in Lemma 1, 2, and 3, respectively.

Lemma 1 (IND-ID-CPA): The advantage of an adversary in winning the IND-ID-CPA Game for the constructed A-IBE is negligible.

Proof: In the IND-tID-CPA game of the constructed A-IBE scheme, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows.

Setup. $\mathcal{C}$ runs Setup to generate a master key pair (mpk, msk) and sends mpk to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ issues adaptive private key queries. For a queried identity ID, $\mathcal{C}$ interacts with $\mathcal{A}$ to run KeyGenPro and lets $\mathcal{A}$ obtain the corresponding private key d_{ID} created with a token t_k. Note that for the same ID, $\mathcal{C}$ guarantees that $\mathcal{A}$ will obtain the same private key.

Challenge. Once $\mathcal{A}$ decides that Phase 1 is over, it submits two different messages M_0^*, M_1^* from the message space and an identity ID^* for challenge.

- If ID^* was not queried in Phase 1, $\mathcal{C}$ picks a random bit $\mu \in \{0, 1\}$ and randomly chooses a token t_c^*, runs Encrypt to generate the challenge ciphertext CT^* with (M_μ^*, t_c^*), and sends CT^* to $\mathcal{A}$.
- Otherwise, ID^* was queried in Phase 1. Let the corresponding private key be d_{ID^*} associated with a token t_k^*. $\mathcal{C}$ sets the token $t_c^* = t_k^*$, picks a random bit $\mu \in \{0, 1\}$, and runs Encrypt to generate the challenge ciphertext CT^* with (M_μ^*, t_c^*). $\mathcal{C}$ then sends CT^* to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ issues more private key queries. For a query on ID, $\mathcal{C}$ responds as follows.

- If $ID = ID^*$ and ID^* was not queried before, $\mathcal{C}$ interacts with $\mathcal{A}$ to run KeyGenPro and lets $\mathcal{A}$ obtain the corresponding private key d_{ID^*} associated with t_k^*, where $t_k^* = t_c^*$.
- Otherwise, $\mathcal{C}$ responds to $\mathcal{A}$ the same as Phase 1.

Guess. Finally, $\mathcal{A}$ outputs its guess μ' of μ and wins the game if $\mu' = \mu$.

It is easy to see that the only difference in the IND-tID-CPA game between the constructed A-IBE scheme and the underlying TB-IBE scheme is the key generation process, where that is a protocol KeyGenPro in the A-IBE scheme but an algorithm T.KeyGen instead in the TB-IBE scheme. As the KG-Replace security, the TB-IBE scheme is still IND-tID-CPA secure when the key generation algorithm T.KeyGen is replaced with the key generation protocol T.KeyGenPro. Since KeyGenPro is the same as T.KeyGenPro, it follows easily that the A-IBE scheme is IND-tID-CPA secure. Then, we have that the A-IBE scheme is IND-ID-CPA secure since the IND-tID-CPA security covers the IND-ID-CPA security (see subsection III-A).

Lemma 2 (Dishonest PKG Security): The advantage of an adversary in winning the Dishonest PKG Game for the constructed A-IBE scheme is negligible.

Proof: In the dishonest PKG game of the constructed A-IBE scheme, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows.

Setup. $\mathcal{A}$ sends mpk and the challenge identity ID^* to $\mathcal{C}$. $\mathcal{C}$ aborts if mpk and ID^* are not well-formed.

KeyGen. $\mathcal{C}$ interacts with $\mathcal{A}$ to run KeyGenPro to generate a well-formed corresponding private key d_{ID^*} associated with a token t_k^* for ID^*. $\mathcal{C}$ sets d_{ID^*} as its secret output.

Query. $\mathcal{A}$ can make decryption queries on adaptively chosen ciphertexts. For a queried ciphertext CT associated with the token t_c, $\mathcal{C}$ runs T.CCheck on CT and aborts if it returns 0. Otherwise, $\mathcal{C}$ runs Decrypt on CT and sends the output $M/\perp$ to $\mathcal{A}$.

Frame. $\mathcal{A}$ outputs an ϵ-useful decoder box $\mathbb{D}$ for ID^* and wins the game if $\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = U$.

If $\mathcal{A}$ wins this game, we have $\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = U$. Which means that in the trace algorithm Trace, $ctr = 0$ at last. Below, we analyze that if the ϵ-useful decoder box $\mathbb{D}$ is generated by PKG, the probability of $ctr = 0$ is negligible.

First, we show that the malicious PKG $\mathcal{A}$ can extract the token t_k^* with negligible probability. In the KeyGen phase, as the KG-Anonymity security, $\mathcal{A}$ has negligible probability in guessing t_k^* in d_{ID^*}. In the Query phase, $\mathcal{A}$ makes decryption queries on adaptively chosen ciphertexts. Since $\mathcal{C}$ will first run the ciphertext sanity check on the queried ciphertext and aborts if the check fails, only well-formed ciphertexts can be accepted to be decrypted. As the decryption of a well-formed ciphertext using well-formed private keys will lead to the same result, $\mathcal{A}$ can extract t_k^* with negligible probability.

Then, since the PKG can only extract the token t_k with negligible probability, the probability that an iteration in the trace algorithm keeps ctr unchanged is at most $1 - \epsilon$. As the ϵ-useful decoder box $\mathbb{D}$ is assumed to be stateless, we have

$$\begin{aligned}\Pr[ctr = 0] &\leq (1-\epsilon)^L \approx exp(-\epsilon L) \\ &= exp(-\epsilon \cdot \lambda/\epsilon) = exp(-\lambda),\end{aligned}$$

which is negligible. Therefore, the advantage of an adversary in winning this game is negligible.

Lemma 3 (Dishonest User Security): The advantage of an adversary in winning the Dishonest User Game for the constructed A-IBE scheme is negligible.

Proof: From Lemma 1, we have that the A-IBE scheme is IND-tID-CPA secure. Next, we give the proof that the IND-tID-CPA security of the A-IBE scheme implies its dishonest user security.

Assume an adversary $\mathcal{A}$ can break the dishonest user security of the A-IBE scheme. We use $\mathcal{A}$ to construct another adversary $\mathcal{B}$ to break the IND-tID-CPA security of the A-IBE scheme as follows.

Setup. The challenger runs the setup algorithm Setup to generate a master key pair (mpk, msk). Then $\mathcal{B}$ is given mpk and gives it to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ makes adaptively private key queries. For a query on ID, $\mathcal{A}$ interacts with $\mathcal{B}$, $\mathcal{B}$ interacts with the challenger to run the key generation protocol KeyGenPro to generate a well-formed corresponding private key d_{ID} with (ID, t_k) by sending sends everything received from $\mathcal{A}$ to the challenger and everything received from the challenger to $\mathcal{A}$. Finally, $\mathcal{A}$ receives d_{ID} as its private key.

Challenge. $\mathcal{B}$ receives a private key d_{ID^*} associated with (ID^*, t_k^*) and an ϵ-useful decoder box $\mathbb{D}^*$ for ID^* from $\mathcal{A}$. $\mathcal{B}$ then sends two different messages M_0^*, M_1^* from the

message space and the identity ID^* to the challenger. Since ID^* has been queried, the challenger chooses a random bit $\mu \in \{0,1\}$, sets the token $t_c^* = t_k^*$, and runs Encrypt to generate the challenge ciphertext CT^* with (ID^*, M_μ^*, t_c^*). The challenger gives CT^* to $\mathcal{B}$.

Phase 2. This phase can be omitted since $\mathcal{B}$ has obtained the decoder box $\mathbb{D}^*$ for the challenge identity ID^*.

Guess. Since $\mathcal{A}$ wins the dishonest user game, we have $\mathsf{Trace}(mpk, d_{ID^*}, \mathbb{D}^*) = PKG$. Which means that taking as input a ciphertext CT encrypted with a token t_k^*, the decoder box $\mathbb{D}$ will output M' such that $M' = M$ at least in one iteration, where t_k^* is the token of the input private key d_{ID^*}. $\mathcal{B}$ feeds CT^* to $\mathbb{D}$, $\mathbb{D}$ will output M_μ^* with the probability $1/L$ as CT^* is associated with the token t_k^*. Since $L = \lambda/\epsilon$ is a polynomial number, we have that $\mathbb{D}^*$ will output M_μ^* with non-negligible probability. $\mathcal{B}$ then checks $M_\mu^* = M_0^*$ or $M_\mu^* = M_1^*$, if the former one holds, $\mathcal{B}$ outputs its guess as $\mu = 0$. Otherwise, if the latter one holds, $\mathcal{B}$ outputs its guess as $\mu' = 1$. The advantage of adversary in guessing μ correctly is non-negligible.

Therefore, if an adversary can break the dishonest user security of an A-IBE scheme, the adversary will break its IND-tID-CPA security with non-negligible probability. As the A-IBE scheme is IND-tID-CPA secure, it is dishonest user secure as well.

This completes the proof of Theorem 1.

IV. A CONCRETE SCHEME

In this section, we give an instantiation of the proposed generic construction based on Park-Lee IBE scheme [4]. In particular, our instantiation achieves adaptive-ID dishonest user security.

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$ and e be a bilinear map, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. If $e(u^a, v^b) = e(u, v)^{ab}$ holds for all $u, v \in \mathbb{G}, a, b \in \mathbb{Z}_p$ and $e(g, g) \neq 1$. We say that $\mathbb{G}$ is a bilinear group if the group operation in $\mathbb{G}$ and the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ are both efficiently computable. Notice that the map e is symmetric since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$. Let $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, g, p, e)$ be the pairing group consists of the objects defined above.

A. PARK-LEE IBE SCHEME

We first show that Park-Lee IBE scheme is a TB-IBE scheme.

- $\mathsf{T.Setup}(1^\lambda)$. Taking as input a security parameter λ, it selects a pairing group $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, g, p, e)$ and a cryptographic hash function $H : \{0,1\}^* \to \mathbb{G}$. Then it randomly chooses $g_2 \in \mathbb{G}, \alpha \in \mathbb{Z}_p$, computes $g_1 = g^\alpha$, and sets a master public/secret key pair $(T.mpk, T.msk)$ as
$$T.mpk = (\mathbb{PG}, g_1, g_2, H),\ T.msk = \alpha.$$
- $\mathsf{T.KeyGen}(T.mpk, T.msk, ID, t_k)$. Taking as input $(T.mpk, T.msk)$ and an identity $ID \in \{0,1\}^*$, it randomly chooses a token $t_k \in \mathbb{Z}_p$ and a number $r \in \mathbb{Z}_p$, computes the corresponding private key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ for ID as
$$\left(g_2^{\alpha+r}, g^r, \left(H(ID)g_2^{t_k}\right)^r, t_k\right).$$
- $\mathsf{T.Encrypt}(T.mpk, ID, M, t_c)$. Taking as input $T.mpk$, an identity $ID \in \{0,1\}^*$, and a message $M \in \mathbb{G}_T$, it randomly chooses a token $t_c \in \mathbb{Z}_p$ and a number $s \in \mathbb{Z}_p$, computes the corresponding ciphertext $T.CT = (C_1, C_2, C_3, C_4)$ as
$$\left(\left(H(ID)g_2^{t_c}\right)^s,\ g^s,\ t_c,\ M \cdot e(g_1, g_2)^s\right).$$
- $\mathsf{T.Decrypt}(T.mpk, T.d_{ID}, T.CT)$. Taking as input $T.mpk$, a private key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ for (ID, t_k), and a ciphertext $T.CT = (C_1, C_2, C_3, C_4)$, it returns $\perp$ if $C_3 = d_4$. Otherwise, it computes M as
$$\begin{aligned}&\frac{C_4}{e(d_1, C_2)} \cdot \frac{e(d_2, C_1)^{\frac{1}{C_3 - d_4}}}{e(d_3, C_2)}\\ =&\frac{M \cdot e(g_1, g_2)^s}{e(g_2^{\alpha+r}, g^s)} \cdot \left(\frac{e(g^r, \left(H(ID)g_2^{t_c}\right)^s)}{e(\left(H(ID)g_2^{t_k}\right)^r, g^s)}\right)^{\frac{1}{t_c - t_k}}\\ =&M.\end{aligned}$$

B. SECURITY PROOF

We now prove that the Park-Lee IBE scheme is IND-tID-CPA secure under the DBDH assumption (suppose $a, b, c, z \in \mathbb{Z}_p$ are randomly chosen numbers, no probabilistic polynomial-time algorithm can distinguish the tuple $(g, g^a, g^b, g^c, e(g, g)^{abc})$ from the tuple $(g, g^a, g^b, g^c, e(g, g)^z)$ with non-negligible advantage).

Note that the IND-tID-CPA security proof of the Park-Lee IBE scheme allows the private key query on the challenge identity ID^*. This leads to two more new problems in the security proof of IND-tID-CPA compared to that of IND-ID-CPA. One is how to simulate the challenge ciphertext CT^* if ID^* was queried in Phase 1. The other one is how to simulate the private key of ID^* in Phase 2 if it was not queried in Phase 1. The core idea of these two simulations is that let the token t_k^* included in the private key of ID^* be as the same as the token t_c^* included in the challenge ciphertext CT^*.

Theorem 2: Suppose the hash function H is a random oracle. The Park-Lee IBE scheme is an IND-tID-CPA secure TB-IBE scheme under the DBDH assumption.

Proof: Suppose there exists an adversary $\mathcal{A}$ who can ε-break the Park-Lee IBE scheme in the IND-tID-CPA security model. We construct a simulator $\mathcal{B}$ to solve the DBDH problem. Given a problem instance $\left(g, g^a, g^b, g^c, Z\right)$ over the pairing group $\mathbb{PG}$, $\mathcal{B}$ runs $\mathcal{A}$ and works as below.

Setup. $\mathcal{B}$ sets the master pubic key as $T.mpk = (\mathbb{PG}, g_1 = g^a, g_2 = g^b)$, where α is implicitly set as a. Let the hash function H be a random oracle.

H-Query. In this phase, $\mathcal{A}$ makes hash queries to the random oracle H on adaptively chosen identities. $\mathcal{B}$ sets a hash list $\mathcal{L}$ to record the respond tuple (ID, t, x, h), where the list is initially empty. For a query on ID, if ID has been recorded in the $\mathcal{L}$ of a tuple (ID, t, x, h), $\mathcal{B}$ returns h to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly chooses $t, x \in \mathbb{Z}_p$, and computes

$$h = H(ID) = g_2^{-t} g^x.$$

Then, $\mathcal{B}$ sends h to $\mathcal{A}$ and adds the tuple (ID, t, x, h) to the hash list $\mathcal{L}$.

Phase 1. In this phase, $\mathcal{A}$ is allowed to adaptively issue private key queries. For a query on ID, let the corresponding hash tuple kept in $\mathcal{L}$ be (ID, t, x, h). $\mathcal{B}$ randomly chooses $r' \in \mathbb{Z}_p$, implicitly sets $r = -a + r'$ and let $t_k = t$, then computes the private key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ as

$$\begin{aligned}
d_1 &= g_2^{\alpha + r} = g_2^{a - a + r'} = (g^b)^{r'}, \\
d_2 &= g^r = g^{-a + r'} = (g^a)^{-1} g^{r'}, \\
d_4 &= t_k = t, \\
d_3 &= \left(H(ID) g_2^t\right)^r = \left(g_2^{-t} g^x g_2^t\right)^{-a + r'} = (g^a)^{-x} g^{x \cdot r'}.
\end{aligned}$$

It is easy to see that $T.d_{ID}$ is a well-formed private key for ID. Then, $\mathcal{B}$ sends the private key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ to $\mathcal{A}$.

Challenge. Once $\mathcal{A}$ decides that Phase 1 is over, it outputs two different messages $M_0^*, M_1^* \in \mathbb{G}_T$ and a challenge identity ID^*, where ID^* could be one of the queried identities in Phase 1. In particular, no matter whether the queried identity is ID^* or not, the simulation for the challenge ciphertext $T.CT^*$ is as follows. let (ID^*, t^*, x^*, h^*) be the corresponding hash tuple in the $\mathcal{L}$ of ID^*. $\mathcal{B}$ randomly picks a bit $\mu \in \{0, 1\}$, sets the token $t_c^* = t^*$, and computes the challenge ciphertext $T.CT^* = (C_1^*, C_2^*, C_3^*, C_4^*)$ as

$$\begin{aligned}
C_1^* &= \left(H(ID^*) g_2^{t_c^*}\right)^s = \left(g_2^{-t^*} g^{x^*} g_2^{t^*}\right)^c = \left(g^c\right)^{x^*}, \\
C_2^* &= g^s = g^c, \\
C_3^* &= t_c^* = t^*, \\
C_4^* &= M_\mu^* \cdot Z = M_\mu^* \cdot e(g, g)^{abc}.
\end{aligned}$$

It is easy to see $T.CT^*$ is a well-formed ciphertext for ID. $\mathcal{B}$ then returns $T.CT^*$ to $\mathcal{A}$.

Phase 2. In this phase, $\mathcal{A}$ is allowed to make more private key queries. $\mathcal{B}$ responds as in Phase 1. Note that the private key for ID^* can be queried in this phase. If ID^* was not queried in Phase 1, $\mathcal{B}$ sets $t_k = t_c^* = t^*$ and generate the corresponding private key d_{ID}^* with the hash tuple (ID^*, t^*, x^*, h^*). The key generation is the same as Phase 1.

Guess. $\mathcal{A}$ outputs its guess μ' of μ. $\mathcal{B}$ outputs 1 if $\mu' = \mu$. Otherwise, $\mathcal{B}$ outputs 0.

Next, we analyze the advantage of $\mathcal{B}$ in solving the DBDH problem as follows. If $Z = e(g, g)^{abc}$ is true, the simulation is indistinguishable from the real attack. According to the assumption that $\mathcal{A}$ can ε-break the scheme, we have the probability of $\mathcal{A}$ in guessing the encrypted message correctly to be $|\Pr[\mu' = \mu | Z = e(g, g)^{abc}]| = 1/2 + \varepsilon$. If Z is random, $T.CT^*$ is a one-time pad since M is encrypted using Z, which is random and unknown in the view of $\mathcal{A}$. In this case, the probability of $\mathcal{A}$ in guessing the encrypted message correctly is $|\Pr[\mu' = \mu] | Z \neq e(g, g)^{abc}| = 1/2$. Then, the advantage of $\mathcal{B}$ in solving the DBDH problem is

$$\begin{aligned}
&\left|\Pr[\mu' = \mu | Z = e(g, g)^{abc}] - \Pr[\mu' = \mu | Z \neq e(g, g)^{abc}]\right| \\
&\quad = |1/2 + \varepsilon - 1/2| \\
&\quad = \varepsilon.
\end{aligned}$$

This completes the proof of Theorem 2.

C. THREE PROPERTIES

Finally, we show that Park-Lee IBE scheme satisfies the required three properties, and hence, it can be converted to a secure A-IBE scheme following the generic construction. First, we give the following two algorithms and one protocol, i.e., a key sanity check algorithm T.KCheck, a ciphertext sanity check algorithm T.CCheck, and a key generation protocol T.KeyGenPro.

- T.KCheck$(T.mpk, T.d_{ID})$: Taking as input $T.mpk$ and a private key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ for ID, it outputs 1 if both the following equations hold.
$$e(d_1, g) = e(g_2, g_1) \cdot e(g_2, d_2)$$
$$e(d_3, g) = e(H(ID), d_2) \cdot e(g_2^{d_4}, d_2)$$
Otherwise, it outputs 0.
- T.CCheck$(T.mpk, T.CT)$: Taking as input $T.mpk$ and a ciphertext $T.CT = (C_1, C_2, C_3, C_4)$ for ID, it outputs 1 if the following equation holds.
$$e(C_1, g) = e(H(ID), C_2) \cdot e(g_2^{C_3}, C_2)$$
Otherwise, it outputs 0.
- T.KeyGenPro$(T.mpk, T.msk, ID)$: PKG takes as input $(T.mpk, T.msk)$ and an identity ID; U takes as input $T.mpk$ and ID; U interacts with the PKG as follows.
  1) U randomly selects $\bar{k}, \bar{t} \in \mathbb{Z}_p$ and runs a zero-knowledge proof (described below) with PKG to prove that $R = H(ID)^{\bar{k}} g_2^{\bar{t}}$.

In the key generation protocol T.KeyGenPro, the user U interacts with the PKG with the zero-knowledge proof described as below. In the proof, U possesses $(H(ID), g_2, \bar{k}, \bar{t}, R)$ and the PKG possesses $(H(ID), g_2, R)$. U wants to convince the PKG that R is computed with $\bar{k}, \bar{t}$ as $R = H(ID)^{\bar{k}} g_2^{\bar{t}}$ without leaking the secret of $\bar{k}, \bar{t}$. The security of this zero-knowledge proof is referred to [20].

2) PKG outputs $\perp$ if the proof fails. Otherwise, it randomly selects $r', t' \in \mathbb{Z}_p$, computes the "partial private key" $T.d'_{ID} = (d'_1, d'_2, d'_3, d'_4)$ as follows, and sends $T.d'_{ID}$ to U.

$$\left(g_2^{\alpha+r'},\ g^{r'},\ \left(Rg_2^{t'}\right)^{r'},\ t'\right)$$

3) U randomly chooses $\bar{r} \in \mathbb{Z}_p$, computes

$$d_1 = d'_1 \cdot g_2^{\bar{r}},\ d_2 = d'_2 \cdot g^{\bar{r}},$$
$$d_3 = {d'_3}^{1/\bar{k}} \left(H(ID) g_2^{d_4}\right)^{\bar{r}},$$
$$d_4 = (\bar{t} + d'_4)/\bar{k}.$$

Let $r = r' + \bar{r}$ and $t_k = (\bar{t} + t')/\bar{k}$. U then sets its decryption key $T.d_{ID} = (d_1, d_2, d_3, d_4)$ as

$$\left(g_2^{\alpha+r},\ g^r,\ \left(H(ID)g_2^{t_k}\right)^r,\ t_k\right).$$

U		PKG
$(H(ID), g_2, \bar{k}, \bar{t}, R)$		$(H(ID), g_2, R)$
Randomly pick $r_1, r_2 \in \mathbb{Z}_p$, Compute $y = H(ID)^{r_1} g_2^{r_2}$	$\xrightarrow{y}$	
		Randomly choose $c \in \mathbb{Z}_p$
	$\xleftarrow{c}$	
Compute $s_1 = r_1 - \bar{k}c$, $s_2 = r_2 - \bar{t}c$		
	$\xrightarrow{s_1, s_2}$	
		Verify if $H(ID)^{s_1} g_2^{s_2} R^c = y$, If so, accept R, Otherwise, reject R

Next, we prove that the constructed key generation protocol is secure, i.e, it satisfies KG-Replace and KG-Anonymity securities.

Theorem 3: The key generation protocol T.KeyGenPro is secure.

Proof: As a secure T.KeyGenPro requires the KG-Replace security and the KG-Anonymity security, we prove these two in Lemma 4 and 5, respectively.

Lemma 4 (KG-Replace Security): The key generation protocol T.KeyGenPro satisfies the KG-Replace security.

Proof: How to issue a private key d_{ID} for an identity *ID* is the only difference in the IND-tID-CPA security proof before and after replacing the key generation algorithm T.KeyGen with the key generation protocol T.KeyGenPro. Let the hash tuple of *ID* in $\mathcal{L}$ be (ID, t, x, h). In the IND-tID-CPA security proof of the Park-Lee IBE scheme, the simulator acting as the PKG sets $t_k = t$ to generate the corresponding private key with (ID, t_k). After being replaced with the key generation protocol, the user and the PKG engage in a key generation protocol where t_k should be jointly determined by both of them (via $\bar{t}$ and t'). In the corresponding security proof, the simulator acting as the PKG only needs to generate a partial private key for the queried *ID*.

Then, if the simulator can successfully simulate the partial private key, we can have the KG-Replace be proved. The simulator $\mathcal{B}$ performs as follows to simulate the partial private key for *ID*.

- Receiving $R = H(ID)^{\bar{k}} g_2^{\bar{t}} = h^{\bar{k}} g_2^{\bar{t}}$ from the adversary $\mathcal{A}$, the simulator $\mathcal{B}$ interacts with $\mathcal{A}$ to run the zero-knowledge proof and aborts if the proof fails. Otherwise, $\mathcal{B}$ randomly chooses $\tilde{r} \in \mathbb{Z}_p$, implicitly sets $r' = -a + \tilde{r}$ and let $t_k = t$, then computes a well-formed private key as the simulation of private keys in IND-tID-CPA security proof for the Park-Lee IBE scheme:

$$\widehat{T.d_{ID}} = (\widehat{d_1}, \widehat{d_2}, \widehat{d_3}, \widehat{d_4}) = \left(g_2^{\alpha+r'}, g^{r'}, (hg_2^{t_k})^{r'}, t_k\right).$$

$\mathcal{B}$ then rewinds $\mathcal{A}$ to obtain ($\bar{k}$ and $\bar{t}$) [1]. It then computes the partial private key $T.d'_{ID}$ as follows and sends it to $\mathcal{A}$.

$$\begin{aligned} T.d'_{ID} &= (d'_1, d'_2, d'_3, d'_4) \\ &= \left(\widehat{d_1}, \widehat{d_2},\ \widehat{d_3}^{\bar{k}},\ \widehat{d_4} \cdot \bar{k} - \bar{t}\right) \\ &= \left(g_2^{\alpha+r'}, g^{r'}, \left((hg_2^{t_k})^{r'}\right)^{\bar{k}}, t_k \cdot \bar{k} - \bar{t}\right) \\ &= \left(g_2^{\alpha+r'}, g^{r'}, (h^{\bar{k}} g_2^{\bar{t}} \cdot g_2^{t_k\bar{k}-\bar{t}})^{r'}, t_k \cdot \bar{k} - \bar{t}\right) \\ &= \left(g_2^{\alpha+r'}, g^{r'}, (R \cdot g_2^{t_k\bar{k}-\bar{t}})^{r'}, t_k \cdot \bar{k} - \bar{t}\right) \end{aligned}$$

Let $t' = t_k \cdot \bar{k} - \bar{t}$, we have

$$T.d'_{ID} = \left(g_2^{\alpha+r'}, g^{r'}, (R \cdot g_2^{t'})^{r'}, t'\right).$$

Therefore, the key generation protocol can be successfully simulated. The key generation protocol T.KeyGenPro satisfies the KG-Replace security.

Lemma 5 (KG-Anonymity Security): The key generation protocol T.KeyGenPro satisfies the KG-Anonymity security.

Proof: In the key generation protocol T.KeyGenPro, U finally obtains a private key $T.d_{ID}$ created with (ID, t_k), where the token t_k is computed by $\bar{t}, \bar{k}$, and t'. As $\bar{t}$ and $\bar{k}$ are protected by the zero-knowledge proof, we have that PKG obtain zero knowledge about t_k. Since the token space is $\mathbb{Z}_p$, PKG has negligible probability in guessing t_k. Therefore, the KG-Anonymity security is satisfied.

This completes the proof of Theorem 3.

With the constructed two algorithms and one protocol above, this completes the proof that the Park-Lee IBE scheme satisfies the Key-Well-Form, Cip-Well-Form, and

KG-Transfer properties. Following Theorem 1, we have that Park-Lee IBE scheme can be converted to an A-IBE scheme which is IND-ID-CPA secure, dishonest PKG secure, and dishonest user secure. Moreover, we can apply the technique developed in [21] to our construction to obtain an IND-ID-CCA secure A-IBE scheme under a random oracle model.

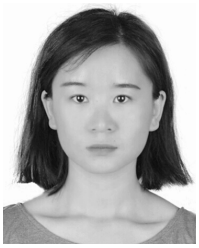
Following the generic construction, the transferred A-IBE scheme using Park-Lee IBE scheme has the same parameter sizes and computational complexity as Park-Lee IBE scheme. Therefore, we can obtain an A-IBE scheme with the constant size master public/secret key pair, private keys, and ciphertexts. Moreover, the computation cost for encryption and decryption in our A-IBE scheme is also constant. The specific size and cost are analyzed as shown in Table 1.

V. CONCLUSION

We proposed a generic construction for full black-box accountable authority identity-based encryption (A-IBE). In comparison with the existing generic constructions which apply the complex and inefficient ABE, our generic construction eliminates the ABE and is built from a variant IBE called token-based identity-based encryption (TB-IBE) with three defined properties, i.e., Key-Well-Form, Cip-Well-Form, and KG-Transfer. We proved that Park-Lee IBE scheme is a secure TB-IBE in the IND-tID-CPA security model defined in this work. Subsequently, we constructed a key sanity check, a ciphertext sanity check, and a secure key generation protocol for Park-Lee IBE scheme to prove that it satisfies the required three properties, and hence, it can be transferred to a full black-box A-IBE scheme. This instantiation is comparable to Park-Lee IBE scheme and more efficient than the existing full black-box A-IBE schemes in terms of parameter sizes (i.e. constant size master public/secret key, private keys, and ciphertexts) and computational complexity (i.e. constant computational complexity for encryption and decryption).

REFERENCES

[1] V. Goyal, "Reducing trust in the PKG in identity based cryptosystems," in *Proc. CRYPTO*, vol. 4622, 2007, pp. 430–447.
[2] V. Goyal, S. Lu, A. Sahai, and B. Waters, "Black-box accountable authority identity-based encryption," in *Proc. CCS*, 2008, pp. 427–436.
[3] A. Sahai and H. Seyalioglu, "Fully secure accountable-authority identity-based encryption," in *Proc. PKC*, vol. 6571, 2011, pp. 296–316.
[4] J. H. Park and D. H. Lee, "An efficient IBE scheme with tight security reduction in the random oracle model," *Des., Codes Cryptogr.*, vol. 79, no. 1, pp. 63–85, 2016.
[5] B. Libert and D. Vergnaud, "Towards black-box accountable authority IBE with short ciphertexts and private keys," in *Proc. PKC*, vol. 5443, 2009, pp. 235–255.
[6] A. Kiayias and Q. Tang, "Making *any* identity-based encryption accountable, efficiently," in *Proc. ESORICS*, vol. 9326, 2015, pp. 326–346.
[7] M. H. Au, Q. Huang, J. K. Liu, W. Susilo, D. S. Wong, and G. Yang, "Traceable and retrievable identity-based encryption," in *Proc. ACNS* Lecture Notes in Computer Science, vol. 5037, 2008, pp. 94–110.
[8] J. Lai, R. H. Deng, Y. Zhao, and J. Weng, "Accountable authority identity-based encryption with public traceability," in *Proc. CT-RSA*, vol. 7779, 2013, pp. 326–342.
[9] J. Li, K. Ren, and K. Kim, "A2BE: Accountable attribute-based encryption for abuse free access control," *IACR Cryptol. ePrint Arch.*, vol. 2009, p. 118, 2009. [Online]. Available: https://dblp.org/rec/bib/journals/iacr/LiRK09
[10] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proc. ASIACCS*, 2011, pp. 386–390.
[11] Z. Liu, Z. Cao, and D. S. Wong, "Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay," in *Proc. CCS*, 2013, pp. 475–486.
[12] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 76–88, Jan. 2013.
[13] J. Ning, Z. Cao, X. Dong, L. Wei, and X. Lin, "Large universe ciphertext-policy attribute-based encryption with white-box traceability," in *Proc. ESORICS* Lecture Notes in Computer Science, vol. 8713. Wroclaw, Poland: Springer, 2014, pp. 55–72.
[14] J. Ning, X. Dong, Z. Cao, and L. Wei, "Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud," in *Proc. ESORICS*, vol. 9327, 2015, pp. 270–289.
[15] Y. Zhang, J. Li, D. Zheng, X. Chen, and H. Li, "Accountable large-universe attribute-based encryption supporting any monotone access structures," in *Proc. ACISP*, vol. 9722, 2016, pp. 509–524.
[16] J. Lai and Q. Tang, "Making any attribute-based encryption accountable, efficiently," in *Proc. ESORICS*, vol. 11099, 2018, pp. 527–547.
[17] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Proc. CRYPTO*, vol. 5677, 2009, pp. 619–636.
[18] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. EUROCRYPT*, vol. 6110, 2010, pp. 62–91.
[19] J. Kim, W. Susilo, F. Guo, and M. H. Au, "A tag based encoding: An efficient encoding for predicate encryption in prime order groups," in *Proc. SCN*, vol. 9841, 2016, pp. 3–22.
[20] J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, Dept. Comput. Sci., ETH Zurich, Zürich, Switzerland, 1998.
[21] E. Fujisaki and T. Okamoto, "How to enhance the security of public-key encryption at minimum cost," in *Proc. PKC*, vol. 1560, 1999, pp. 53–68.



ZHEN ZHAO received the B.S. degree from Shandong Jianzhu University, China, in 2013, and the M.S. degree from Xidian University, China, in 2016, where she is currently pursuing the Ph.D. degree. She has applied for the visiting research program with the University of Wollongong, Australia, from 2017 to 2019. Her major research interests include public-key cryptography; in particular, security proof, and signature and encryption schemes.

JIANCHANG LAI received the Ph.D. degree from the University of Wollongong, Australia, in 2018. He is currently with the School of Computer Science and Technology, Nanjing Normal University. His major research interests include public-key cryptography, including encryption, security proof, and privacy preserving.

WILLY SUSILO (SM'01) received the Ph.D. degree in computer science from the University of Wollongong, Australia, where he is currently a Professor and the Head of the School of Computing and Information Technology. He is also the Director of the Centre for Computer and Information Security Research, University of Wollongong. His main research interests include cloud security, cryptography, and information security. He has served as a Program Committee Member in major international conferences. He has been awarded the prestigious ARC Future Fellow by the Australian Research Council.

BAOCANG WANG received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in cryptography from Xidian University, in 2001, 2004, and 2006, respectively, where he is currently a Professor with the School of Telecommunications Engineering. His main research interests include public key cryptography, wireless network security, and data mining.

YUPU HU received the M.S. degree in mathematics and the Ph.D. degree in cryptology from Xidian University, Xi'an, China, in 1987 and 1999, respectively, where he is currently a Professor with the Telecommunication College. He is also serving as one of the directors of the Chinese Association for Cryptologic Research. His major research interests include cryptology, including stream ciphers, block ciphers, and public key ciphers.

FUCHUN GUO received the B.S. and M.S. degrees from Fujian Normal University, China, in 2005 and 2008, respectively, and the Ph.D. degree from the University of Wollongong, Australia, in 2013, where he is currently an Associate Research Fellow with the School of Computing and Information Technology. His primary research interests include the public-key cryptography, in particular protocols, encryption and signature schemes, and security proof.