PLOS ONE

RESEARCH ARTICLE

Heterogeneous deniable authenticated encryption for location-based services

Chunhua Jin*, Ge Kan, Guanhua Chen, Changhui Yu, Ying Jin, Chengjie Xu

Faculty of Computer & Software Engineering, Huaiyin Institute of Technology, Huai'an, China

* xajch0206@163.com

Abstract

The location-based services can provide users with the requested location information. But users also need to disclose their current location to the location-based service provider. Therefore, how to protect user's location privacy is a major concern. In this paper, we propose a heterogeneous deniable authenticated encryption scheme called HDAE for location-based services. The proposed scheme permits a sender in a public key infrastructure environment to transmit a message to a receiver in an identity-based environment. Our design utilizes a hybrid encryption method combing the tag-key encapsulation mechanism (tag-KEM) and the data encapsulation mechanism (DEM), which is well adopted for location-based services applications. We give how to design an HDAE scheme utilizing a heterogeneous deniable authenticated tag-KEM (HDATK) and a DEM. We also construct an HDATK scheme and provide security proof in the random oracle model. Comprehensive analysis shows that our scheme is efficient and secure. In addition, we give an application of the HDAE to a location-based services system.

OPEN ACCESS

Citation: Jin C, Kan G, Chen G, Yu C, Jin Y, Xu C (2021) Heterogeneous deniable authenticated encryption for location-based services. PLoS ONE 16(1): e0244978. https://doi.org/10.1371/journal.pone.0244978

Editor: Hua Wang, Victoria University, AUSTRALIA

Received: September 11, 2020

Accepted: December 21, 2020

Published: January 6, 2021

Data Availability Statement: All relevant data are within the manuscript and its Supporting information files.

Funding: This research was funded by the Industry University Research of Jiansu Province (grant no. BY2019161), the Natural Science Research in Colleges and Universities of Jiansu Province (grant no. 19KJB510020).

Competing interests: The authors have declared that no competing interests exist.

Introduction

The fast expansion of smart devices and mobile networks makes location-based services (LBSs) an integral part of people's daily lives. Users utilize LBSs to find points of interests, navigate the destination, and inquire public transportation etc. [1–6]. In all of these requested services, users need to disclose their location information to the location-based service provider (LBSP). Based on location information, LBSP is able to infer some sensitive information about users, such as preferences, social circles, and trajectories. For example, if a user frequently presents location request to the same hospital, the LBSP is able to deduce that the user may have a physical issue.

If the LBSP cooperates with a malicious adversary for pecuniary advantage, there will be significant loss of profits for users. For example, based on the location-based privacy information leaked by a user, a malicious adversary can infer a user's home address or routine and then commit theft, which seriously threatens user's personal and property safety. Therefore, protecting users' location privacy is a major concern.

Authentication plays a very important role in the LBS [7–16]. Only authorized users can access the LBS. Typically, we utilize digital signature technology to achieve authentication.

However, there is also non-repudiation in digital signature. That is, the sender cannot deny the message he/she signed. To resolve this issue, deniable authentication [17] is proposed which has two characteristics: (1) the receiver has the capability of identifying whether a given message is from the sender; (2) any third party is incapable of determining whether the given message is from the sender or the receiver even though the third party colludes with the receiver since the receiver is able to generate a probabilistically indistinguishable transcript from the sender. However, in privacy-preserving scenarios, the transmitted message needs to be encrypted to achieve confidentiality. Wu and Li [18] first presented an identity-based DAE scheme to achieve confidentiality as well as deniable authentication in an efficient approach.

0.1 Motivation and contribution

In order to make the designed scheme more practical, we require the sender and receiver to be in different cryptographic environments. Concretely, we design a heterogeneous deniable authenticated encryption (HDAE) scheme utilizing tag-KEM and DEM hybrid encryption methods. The proposed scheme permits a sender in a public key infrastructure (PKI) setting to deliver a message to a receiver in an identity-based cryptography (IBC) setting. This construction provides security proof in random oracle model (ROM) under the DBDH and BDH assumptions. Our experimental analysis displays that our scheme has a high efficiency and security. Additionally, we design an LBS scheme utilizing our proposed HDAE scheme. On the one hand, it permits the LBSP to affirm whether the ciphertext of the submitted location request is from the user. On the other hand, any third party cannot determine whether the ciphertext of the submitted location request is from the user or the service provider even though the third party colludes with the LBSP since the LBSP has the capability of generating a probabilistically indistinguishable ciphertext from the user.

0.2 Organization

The rest of this paper is arranged below. Section II, Related work is presented. Problem formulation is defined in Section III. We design a formal model for the HDAE in Section IV. Section V, a security model for the HDATK is depicted. An HDAE design is presented in Section VI, and we design an HDATK scheme in Section VII. Performance analysis is discussed in Section VIII. Section IX, we give an HDAE application to the LBS. Conclusion is drawn in Section X.

1 Related work

Related notions, hybrid encryption, deniable authenticated encryption, and heterogeneous deniable authentication are introduced.

Hybrid encryption constitutes a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM). The KEM encrypts a session key by a public key, whereas the DEM encrypts the real data by a session key. For large messages, hybrid encryption is the best choice. Cramer and Shoup [19] designed practical and provably secure hybrid KEM/DEM schemes. Abe et al. [20] put forward to a more efficient tag-KEM/DEM scheme. Then, many KEM/DEM schemes [21–28] have been proposed. These designs support both components modular design. Sahai et al. [29] put forward to a tag-KEM/DEM scheme by a non-interactive proof method. The proposed scheme can encrypt message with arbitrary length. Baek et al. [30] presented a stateful KEM-DEM scheme. It is highly effective by utilizing a state to produce the random parameters.

Deniable authentication encryption (DAE) is a cryptographic primitive which can accomplish concurrently public key encryption and deniable authentication. Its cost is lower than that needed by deniable authentication-then-encryption manner. The DAE can achieve deniable authentication and confidentiality simultaneously which is well adopted for privacy-protecting scenarios.

Li et al. [31] constructed a DAE scheme with formal security proof. They also constructed an email system based on the designed DAE scheme. Jin et al. [32] constructed a DAE scheme which can realize simultaneously deniable authentication, confidentiality, and ciphertext anonimity. Rasmussen and Gasti [33] proposed a DAE based on two encryption schemes with strong and weak properties. Recently, Huang et al. [34] constructed a DAE scheme for privacy protection with formal security proof. The above mentioned schemes are all in the PKI environment which has public key management problems, including distribution, storage, and revocation. To resolve this issue, a number of identity-based deniable authenticated encryption (IBDAE) schemes have been constructed. Wu and Li [18] constructed an IBDAE scheme which provided formal security proof. Li et al. [35] (denoted by LZJ) proposed an IBDAE scheme for e-mail system. In their scheme, they utilize tag-KEM/DEM hybrid encryption technology which is more suitable for actual applications. Jin and Zhao [36] designed an IBDAE scheme which admitted formal security proof. The aforementioned schemes have key escrow problems, i.e., a third party called private key generator (PKG) knows all user's private key. To avoid this problem, a certificateless deniable authenticated encryption (CLDAE) scheme [37] has been designed. Recently, Chen et al. [38] proposed a certificateless hybrid KEM/DEM scheme. It separates two parts to provide better security and efficiency.

The aforementioned DAE schemes have a common feature, i.e., the entities of these schemes are all in the same cryptosystem. Such characteristic makes these schemes not well suitable for the LBS system. Li et al. [39] (denoted by LHO) designed two heterogeneous deniable authentication (HDA) schemes. Their designed schemes allowed batch verification to accelerate the authenticators' verification. Jin et al. [40] constructed an HDA scheme. In their scheme, a sender in a CLC setting delivered a message to a receiver in an IBC setting. However, these schemes do not achieve confidentiality.

2 Problem formulation

2.1 System and security models

There are three entities in the HDAE as shown in Fig 1: a user, an LBSP, and a trusted third party PKG. The location information and the corresponding ciphertext are produced by the user, and the ciphertext are sent to the LBSP. The LBSP can identify the received ciphertext is from the user and generate a probabilistically indistinguishable ciphertext from the user. The PKG is mainly responsible for generating system parameters and LBSP's private key.

To obtain the location-based service that supports privacy-preserving, in the proposed system model, the user sends the ciphertext of location-requested information to the LBSP. Then the LBSP decrypts the received ciphertext and checks whether the decrypted message is location-requested information or a failure symbol $\perp$.

2.2 Threat model and security goals

We define an adversary which will act as a user to learn the requested location information of other users. The LBSP is honest-but-curious. It means that it follows the designed scheme, but it may collude with a third party for economic benefits. Additionally, the collusion attack between the LBSP and a third party is concerned in the proposed security goals. Specially, two kinds of security requirements are considered in the constructed scheme.

- Confidentiality: Any information about the submitted location information of a ciphertext cannot be learned by any third party other than the involved entities;

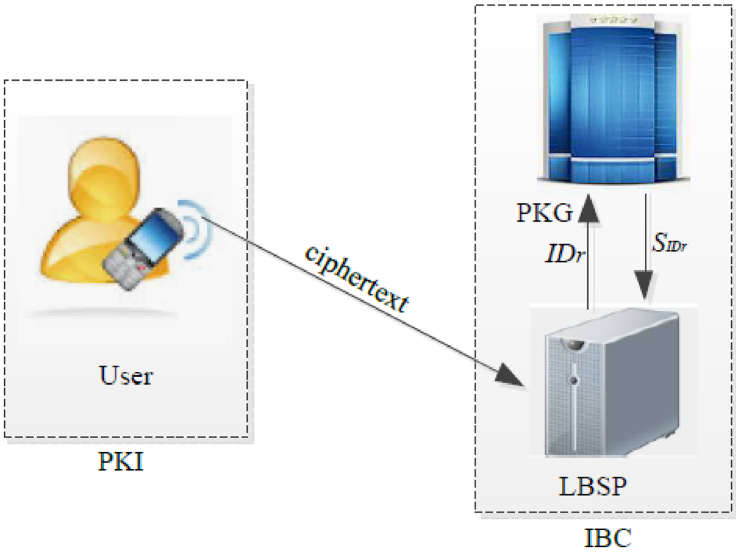


Fig 1. System model.

https://doi.org/10.1371/journal.pone.0244978.g001

- Deniable authentication: The LBSP has a capability of determining a ciphertext is from the user and creating a ciphertext that is probabilistically indistinguishable from the user.

3 PI-HDAE

We describe security notions for the HDAE in this section. In the designed HDAE scheme, a sender in a PKI environment, while a receiver in an IBC environment. PI-HDAE is denoted by this kind of DAE as follows.

3.1 Syntax

A PI-HDAE scheme comprises five algorithms below:

Setup: Given system parameter 1^k, the PKG obtains the *params* and a master private key *s*. In other algorithms, we neglect *params* due to they are public.

PKI-KG: A user belongs to the PKI setting elects a secret key *sk* and calculates its public key *pk*.

IBC-KE: A user in the IBC setting transmits its identity *ID* to the PKG who computes its private key S_{ID} and securely passes it to the user. Here, let the user's public key be its identity *ID*.

Deniable-Authenticated-Encrypt(DAE): Given a message *m*, a sender's secret key sk_s, public key pk_s, and a receiver's identity ID_r, the sender obtains a ciphertext σ.

Deniable-Authenticated-Decrypt(DAD): Given a ciphertext σ, a sender's public key pk_s, a receiver's identity ID_r, and its private key S_{ID_r}, the receiver obtains a message *m* or a symbol $\perp$.

If $\sigma = DAE(m, sk_s, pk_s, ID_r)$, then $m = DAD(\sigma, pk_s, ID_r, S_{ID_r})$.

3.2 Security notions

We rewrite the notions [35] to meet our scheme. For confidentiality, the standard security concept, indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) is employed in our construction.

For IND-CCA2 security in a PI-HDAE scheme, it is assumed that this game below is between an adversary $\mathcal{F}$ with its challenger $\mathcal{C}$.

"IND-CCA2" game (Game-I):

Setup. $\mathcal{C}$ performs *Setup* algorithm to get *params*, releases it to $\mathcal{F}$ and saves s. $\mathcal{C}$ also executes the PKI-KG algorithm to obtain a sender's private/public key pair (sk_s^*, pk_s^*). Then it passes pk_s^* to $\mathcal{F}$.

Phase 1. $\mathcal{F}$ adaptively issues the queries below.

- Key extraction queries: $\mathcal{F}$ picks an identity ID. $\mathcal{C}$ obtains the private key S_{ID} by running an IBC-KE algorithm and transmits it to $\mathcal{F}$.
- DAE queries: $\mathcal{F}$ selects a receiver's identity ID_r, and a message m. Then $\mathcal{C}$ executes DAE(m, sk_s^*, pk_s^*, ID_r) and transmits the result σ to $\mathcal{F}$.
- DAD queries: $\mathcal{F}$ selects a ciphertext σ, and a receiver's identity ID_r. $\mathcal{C}$ obtains S_{ID_r} by implementing key extraction algorithm. It then transmits σ = DAD(σ, pk_s^*, ID_r, S_{ID_r}) to $\mathcal{F}$ (the resulting $\perp$ indicates σ is invalid).

Challenge. $\mathcal{F}$ determines when Phase 1 ends. $\mathcal{F}$ creates a challenge identity ID_r^* and two messages (m_0, m_1). In phase 1, it does not support to request a key extraction query on ID_r^*. $\mathcal{C}$ randomly picks $b \in \{0, 1\}$, computes σ^* = DAE(m_b, sk_s^*, pk_s^*, ID_r) and outputs σ^* to $\mathcal{F}$.

Phase 2. $\mathcal{F}$ makes queries as in Phase 1 except it neither requests a key extraction query on identity ID_r^* nor executes a DAD query on (σ^*, pk_s^*, ID_r^*).

Guess. $\mathcal{F}$ returns b', and it wins the game if $b' = b$.

$\mathcal{F}$'s advantage is

$$Adv_{PI-HDAE}^{IND-CCA2}(\mathcal{F}) = |2Pr[b' = b] - 1|,$$

where $Pr[b' = b]$ expresses the probability.

Definition 1. A PI-HDAE scheme is IND-CCA2 secure if there is a probabilistic polynomial time (PPT) adversary $\mathcal{F}$ wins "IND-CCA2" game with a negligible advantage.

In the aforementioned definition, $\mathcal{F}$ is permitted to gain the sender's private key S_{ID_s} [41]. Namely, the confidentiality is retained if the S_{ID_s} is compromised.

For deniable authentication, the security concept, deniable authentication against adaptive chosen message attacks (DA-CMA) is employed in our construction.

For DA-CMA in a PI-HDAE scheme, this game below is between $\mathcal{F}$ and $\mathcal{C}$.

"DA-CMA" game (Game-II):

Setup. This is identical to Game-I.

Attack. This is identical to Game-I.

Forgery. $\mathcal{F}$ creates a pair (σ^*,ID_r^*). $\mathcal{F}$ succeeds if the conditions below are satisfied:

1. DAD(σ^*,pk_s^*,ID_r^*,S_{ID_r}) = m^*.
2. $\mathcal{F}$ has not issued a key extraction query on ID_r^*.
3. $\mathcal{F}$ has not issued a DAE query on (m^*, ID_r^*).

$\mathcal{F}$'s advantage is defined as the probability that it will win.

Definition 2. A PI-HDAE scheme is DA-CMA secure if there is a PPT adversary $\mathcal{F}$ wins the "DA-CMA" game with a negligible advantage.

In the aforementioned definition, $\mathcal{F}$ does not issue a key extraction query on the identity ID_r^*. This is for deniability. In other words, the two parties involved communication are able to produce a transcript with indistinguishable probability.

3.3 Data Encapsulation Mechanism (DEM)

Two algorithms are included in a DEM.

- Enc: Given 1^k, a message m, and a key K, this algorithm outputs a ciphertext c. It is denoted as $c = Enc(K, m)$.
- Dec: Given a key K, and a ciphertext c, this algorithm outputs a message m or $\perp$.

For a DEM, the security concept, indistinguishability against passive attackers (IND-PA) is employed in our construction. The game below is between $\mathcal{A}$ and $\mathcal{C}$.

IND-PA game (Game-III):

Setup. $\mathcal{A}$ transmits two messages (m_0, m_1).

Challenge. $\mathcal{C}$ picks $K, \beta \in \{0, 1\}$, and outputs a challenge ciphertext $c^* = Enc(K, m_\beta)$ to $\mathcal{A}$.

Guess. $\mathcal{A}$ returns β', and it will win the game if $\beta' = \beta$.

$\mathcal{A}$'s advantage is

$$Adv_{DEM}^{IND-PA}(\mathcal{A}) = |2Pr[\beta' = \beta] - 1|,$$

where $Pr[\beta' = \beta]$ expresses the probability.

Definition 3. A DEM is DA-CPA secure if there is a PPT adversary $\mathcal{A}$ wins "DA-CPA" game with a negligible advantage.

4 PI-HDATK

The security notions for heterogeneous deniable authenticated tag-KEM (HDATK) are given in this section. In the designed HDATK scheme, a sender belongs to a PKI setting, while a receiver belongs to an IBC setting. PI-HDATK is denoted by this kind of DATK scheme as follows.

4.1 Syntax

A PI-HDATK scheme comprises six algorithms below:

Setup: Given 1^k, the PKG obtains the *params* and a master private key s. Due to *params* are public, we neglect them in other algorithms.

PKI-KG: A user in the PKI setting calculates a secret/public key pair (sk, pk).

IBC-KE: A user in the IBC setting transmits its identity ID to the PKG who computes its private key S_{ID} and securely transmits it to the user. Here, we assume that the user's public key is its identity ID.

Sym: Given a sender's secret key sk_s, public key pk_s, and a receiver's identity ID_r, the sender produces an encryption key K and state information ω.

Encap: Given a tag τ and the state information ω, the sender creates an encapsulation ϕ.

Decap: Given a sender's public key pk_s, a receiver's identity ID_r, private key S_{ID_r}, a tag τ, and an encapsulation ϕ, the receiver outputs K or $\perp$.

If $(k, \omega) = Sym(sk_s, pk_s, ID_r)$ and $\phi = Encap(\omega, \tau)$, then $K = Decap(\phi, \tau, pk_s, ID_r, S_{ID_r})$.

4.2 Security notions

The confidentiality and deniable authentication should be satisfied for the PI-HDATK scheme. For IND-CCA2 security in a PI-HDATK scheme, it is assumed that this game below is between $\mathcal{F}$ and $\mathcal{C}$.

"IND-CCA2" game (Game-IV):

Setup. $\mathcal{C}$ performs *Setup* algorithm, delivers *params* to $\mathcal{F}$ and saves *s*. $\mathcal{C}$ also executes PKI-KG algorithm to obtain a sender's private/public key pair (sk_s^*, pk_s^*). Then it delivers pk_s^* to $\mathcal{F}$.

Phase 1. $\mathcal{F}$ adaptively issues queries below.

- Key extraction queries: This is identical to Game-I.
- Symmetric key generation queries: $\mathcal{F}$ submits a receiver's identity ID_r to $\mathcal{C}$. $\mathcal{C}$ then performs $(K, \omega) = Sym(sk_s^*, pk_s^*, ID_r)$, stores the state information ω, and sends the key K to $\mathcal{F}$.
- Encapsulation queries: $\mathcal{F}$ picks a tag τ. If ω is not matched, $\mathcal{C}$ outputs $\perp$. If matched, $\mathcal{C}$ deletes the exist one and produces $\phi = Encap(\omega, \tau)$
- Decapsulation queries: $\mathcal{F}$ picks an encapsulation ϕ, a receiver's identity ID_r, and a tag τ. $\mathcal{C}$ produces S_{ID_r} by performing key extraction algorithm. It outputs the result of Decap(ϕ, τ, pk_s^*, ID_r, S_{ID_r}) to $\mathcal{F}$.

Challenge. $\mathcal{F}$ determines when Phase 1 is over. $\mathcal{F}$ then outputs a challenge identity ID_r^*. In phase 1, it does not support to request a key extraction query on ID_r^*. $\mathcal{C}$ executes (K_1, ω^*) = Sym(sk_s^*,pk_s^*,ID_r^*), picks $b \in \{0, 1\}$, $K_0 \in \mathcal{K}_{\mathcal{PI-HDATK}}$, and passes K_b to $\mathcal{F}$. when $\mathcal{F}$ obtains K_b, it will issue the identical queries as before. $\mathcal{F}$ then returns a tag τ^*. $\mathcal{C}$ calculates a challenge encapsulation ϕ^* = Encap(ω^*, τ^*) and outputs it to $\mathcal{F}$.

Phase 2. $\mathcal{F}$ makes queries as in Phase 1 except it neither requests a key extraction query on identity ID_r^* nor executes a decapsulation query on (ϕ^*, τ^*, pk_s^*, ID_r^*).

Guess. $\mathcal{F}$ returns b', and it wins the game if $b' = b$.

$\mathcal{F}$'s advantage is

$$Adv_{PI-HDATK}^{IND-CCA2}(\mathcal{F}) = |2Pr[b' = b] - 1|,$$

where $Pr[b' = b]$ expresses the probability.

Definition 4. A PI-HDATK scheme is IND-CCA2 secure if a PPT adversary $\mathcal{F}$ wins "IND-CCA2" game with negligible advantage.

In the above definition, it is allowed that $\mathcal{F}$ gets the sender's secret key S_{ID_s}. Namely, the confidentiality is maintained if S_{ID_s} is compromised.

For deniable authentication, the security concept, deniable authentication against adaptive chosen message attacks (DA-CMA) is employed in our design.

For DA-CMA security in a PI-HDATK scheme, it is assumed that this game below is played between $\mathcal{F}$ with $\mathcal{C}$.

"DA-CMA" game(Game-V):

Setup. This is identical to Game-III.

Attack. This is identical to Game-III.

Forgery. $\mathcal{F}$ creates an element (ϕ^*, τ^*, ID_r^*). $\mathcal{F}$ succeeds if the contexts below are met:

1. DAD(σ^*,pk_s^*,ID_r^*) = m^*.
2. $\mathcal{F}$ has not issued a key extraction query on ID_r^*.
3. $\mathcal{F}$ has not issued a DAE query on (m^*, ID_r^*).

$\mathcal{F}$'s advantage is defined as the probability that it will win.

Definition 5. A PI-HDATK scheme is DA-CMA secure if a PPT adversary $\mathcal{F}$ wins the "DA-CMA" game with a negligible advantage.

In the aforementioned definition, $\mathcal{F}$ does not issue a key extraction query on ID_r^*. This is for deniability. That is, the two parties involved communication are able to produce an indistinguishable transcript.

5 A hybrid PI-HDAE scheme

Fig 2 depicts a hybrid PI-HDAE scheme that constitutes a PI-HDATK and a DEM. In DEM part, the ciphertext is a tag. This construction provides simple description. Theorems 1 and 2 present the security consequences.

Theorem 1. Let a hybrid PI-HDAE scheme constitute a PI-HDATK and a DEM which are IND-CCA2 and IND-CPA secure, respectively, PI-HDAE is IND-CCA2 secure. to be specific, we receive

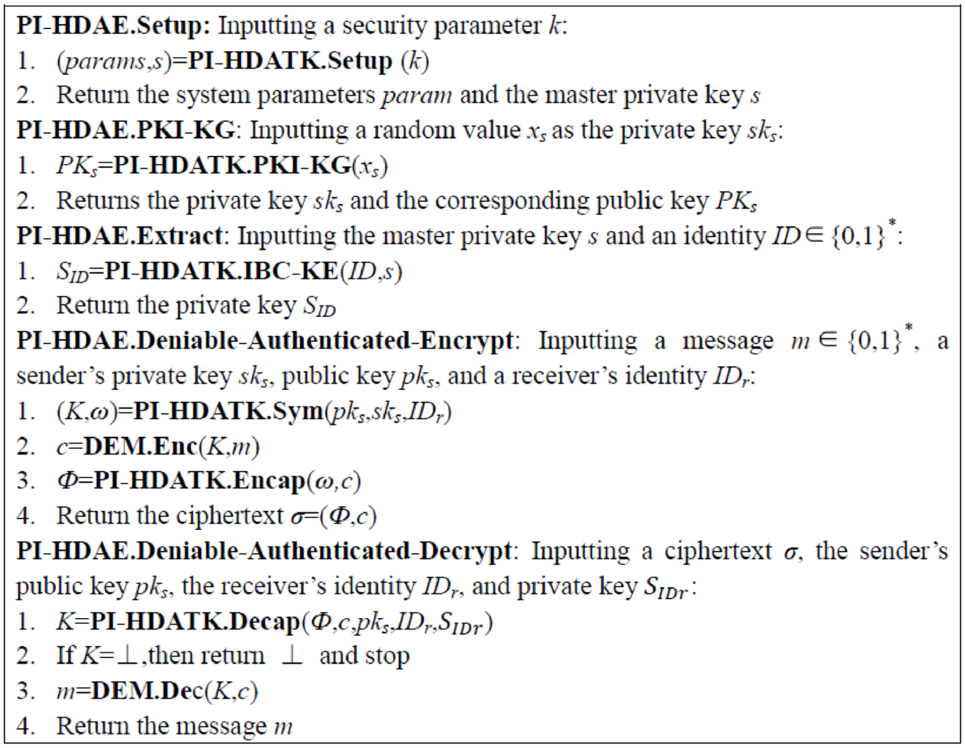
$$Adv_{PI-HDAE}^{IND-CCA2}(\mathcal{F}) = Adv_{PI-HDATK}^{IND-CCA2}(\mathcal{C}_1) + Adv_{DEM}^{IND-PA}(\mathcal{C}_2),$$

Proof: See Appendix 1.

Theorem 2. Let a PI-HDAE constitutes a PI-HDATK and a DEM. If PI-HDATK is DA-CMA secure, PI-HDAE is also DA-CMA secure. to be specific, we receive

$$Adv_{PI-HDAE}^{DA-CMA}(\mathcal{F}) \leq Adv_{PI-HDATK}^{DA-CMA}(\mathcal{C}),$$

Proof: Refer to Appendix 2.



```
PI-HDAE.Setup: Inputting a security parameter $k$:
1. $(params,s)$=PI-HDATK.Setup $(k)$
2. Return the system parameters $param$ and the master private key $s$
PI-HDAE.PKI-KG: Inputting a random value $x_s$ as the private key $sk_s$:
1. $PK_s$=PI-HDATK.PKI-KG$(x_s)$
2. Returns the private key $sk_s$ and the corresponding public key $PK_s$
PI-HDAE.Extract: Inputting the master private key $s$ and an identity $ID \in \{0,1\}^*$:
1. $S_{ID}$=PI-HDATK.IBC-KE$(ID,s)$
2. Return the private key $S_{ID}$
PI-HDAE.Deniable-Authenticated-Encrypt: Inputting a message $m \in \{0,1\}^*$, a sender's private key $sk_s$, public key $pk_s$, and a receiver's identity $ID_r$:
1. $(K,\omega)$=PI-HDATK.Sym$(pk_s,sk_s,ID_r)$
2. $c$=DEM.Enc$(K,m)$
3. $\Phi$=PI-HDATK.Encap$(\omega,c)$
4. Return the ciphertext $\sigma=(\Phi,c)$
PI-HDAE.Deniable-Authenticated-Decrypt: Inputting a ciphertext $\sigma$, the sender's public key $pk_s$, the receiver's identity $ID_r$, and private key $S_{IDr}$:
1. $K$=PI-HDATK.Decap$(\Phi,c,pk_s,ID_r,S_{IDr})$
2. If $K=\perp$,then return $\perp$ and stop
3. $m$=DEM.Dec$(K,c)$
4. Return the message $m$
```

Fig 2. Construction of PI-HDAE from PI-HDATK and DEM.

https://doi.org/10.1371/journal.pone.0244978.g002

6 A PI-HDATK scheme

There are six algorithms to describe our proposed scheme. Fig 3 shows the main description. In DEM part, a tag is the ciphertext. This construction provides simple description and realizes better universal security.

6.1 Basic knowledge

In this section, we provide bilinear pairings properties, decisonal bilinear Diffie-Hellman problem (DBDHP), and bilinear Diffie-Hellman problem (BDHP).

Let G_1, G_2 be an additive group and a multiplicative group, respectively. P is a generator of G_1, and G_1 as well as G_2 have the same prime order q. A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in \mathbb{Z}_q^*$.
2. Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$

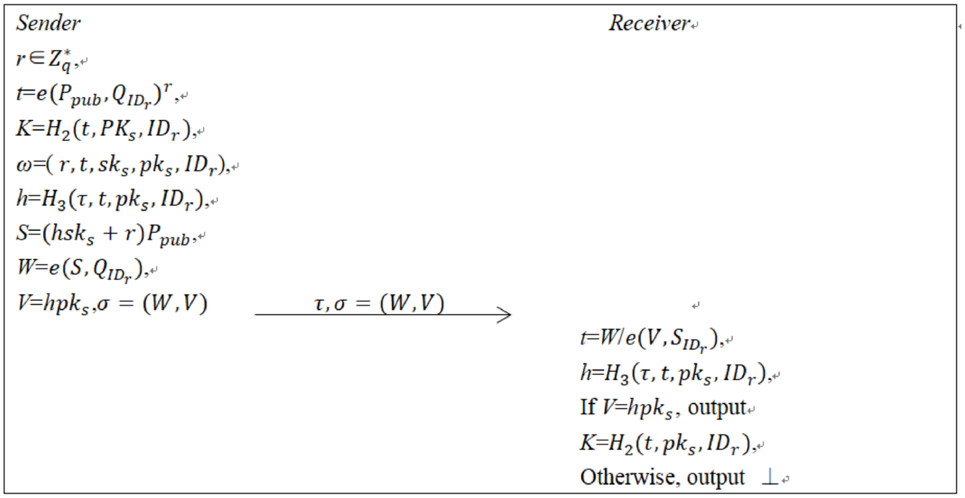
The modified Weil and Tate pairings are the admissible maps ([42–48] offer more information). This scheme's security depends on the difficulty of dealing with the flllowing problems.

Definition 1. Decisional Bilinear Diffie-Hellman Problem (DBDHP). In the light of bilinear pairings basic definition as above mentioned, DBDHP is to determine $\theta = e(P, P)^{abc}$ given (P, aP, bP, cP) with $a, b, c, \theta \in \mathbb{Z}_q^*$.

Definition 2. Bilinear Diffie-Hellman Problem (BDHP). In the light of bilinear pairings basic definition as above mentioned, BDHP is to calculate $e(P, P)^{abc}$ given (P, aP, bP, cP) with $a, b, c \in \mathbb{Z}_q^*$.

6.2 Our scheme

Setup. Given G_1, G_2, P, and e as in Subsection A of Section VII. Let k be a security parameter ($q \geq 2^k$) and n be a a DEM's key length. H_1, H_2, H_3 are three cryptographic hash functions, where H_1: $\{0, 1\}^* \rightarrow G_1$, H_2: $\{0, 1\}^* \times G_1 \times G_2 \rightarrow \{0, 1\}^n$ and $H_3 : \{0,1\}^* \times G_1 \times G_2 \rightarrow \mathbb{Z}_q^*$. The KGC randomly selects a master key $s \in \mathbb{Z}_q^*$ and calculates $P_{pub} = sP$. The public *params* are (G_1, G_2, e, q, n, k, P, P_{pub}, H_1, H_2, H_3) and a master private key is s.



Sender

$r \in Z_q^*$,

$t = e(P_{pub}, Q_{ID_r})^r$,

$K = H_2(t, PK_s, ID_r)$,

$\omega = (r, t, sk_s, pk_s, ID_r)$,

$h = H_3(\tau, t, pk_s, ID_r)$,

$S = (hsk_s + r)P_{pub}$,

$W = e(S, Q_{ID_r})$,

$V = hpk_s, \sigma = (W, V)$

$\xrightarrow{\tau, \sigma = (W, V)}$

Receiver

$t = W / e(V, S_{ID_r})$,

$h = H_3(\tau, t, pk_s, ID_r)$,

If $V = hpk_s$, output

$K = H_2(t, pk_s, ID_r)$,

Otherwise, output $\perp$

Fig 3. The main contribution of PI-HDATK.

https://doi.org/10.1371/journal.pone.0244978.g003

PKI-KG. A user belongs to a PKI setting elecets $x_i \in Z_q^*$ randomly as its secret key sk_i, and calculates $pk_i = sk_i P$ as its public key. Here, $i = s$ denotes the sender, and $pk_s = x_s P$, $sk_s = x_s$ denotes the sender's public/private key pair.

IBC-KE. A user belongs to an IBC setting gives its identity ID to the PKG. The PKG calculates its private key $SK_{ID} = sQ_{ID}(Q_{ID} = H_1(ID))$ and securely transmits it to the user. Here, ID_r denotes the receiver, and $pk_r = ID_r$ $sk_r = S_{ID_r}$ denote the receiver's public and private key.

Sym. Given a sender's private/public key pair (sk_s, pk_s), and a receiver's identity ID_r, the algorithm below is done.

1. Pick $r \in \mathbb{Z}_q^*$.
2. Compute $t = e(P_{pub}, Q_{ID_r})^r$.
3. Calculate $K = H_2(t, pk_s, ID_r)$.
4. Return K and $\omega = (r, t, sk_s, pk_s, ID_r)$.

Encap. Given a tag τ and the state information ω, the algorithm below is done.

1. Compute $h = H_3(\tau, t, pk_s, ID_r)$.
2. Compute $S = (hsk_s + r)P_{pub}$.
3. Compute $W = e(S, Q_{ID_r})$.
4. Compute $V = hpk_s$.
5. Compute $\sigma = (W, V)$.

Decap. Given a tag τ, an encapsulation σ, a sender's public key pk_s, a receiver's private key S_{ID_r}, identity ID_r, the algorithm below is executed.

1. Compute $t = W/e(V, S_{ID_r})$.
2. Compute $h = H_3(\tau, t, pk_s, ID_r)$.
3. If $V = hpk_s$, output $K = H_2(t, pk_s, ID_r)$; if not, return the symbol $\perp$.

The consistency of the designed HDATK scheme can be verified. Because $W = e(S, Q_{ID_r})$, $V = hpk_s$, we can get

$$\begin{array}{rcl} t & = & W/e(V, S_{ID_r}) = e(S, Q_{ID_r})/e(hpk_s, S_{ID_r}) \\ & = & e((hx_s + r)P_{pub}, Q_{ID_r})/e(hpk_s, sQ_{ID_r}) \\ & = & e(hx_sP_{pub}, Q_{ID_r})e(rP_{pub}, Q_{ID_r})/e(hx_ssP, Q_{ID_r}) \\ & = & e(hx_ssP, Q_{ID_r})e(rP_{pub}, Q_{ID_r})/e(hx_ssP, Q_{ID_r}) \\ & = & e(P_{pub}, Q_{ID_r})^r \end{array}$$

6.3 Security

Theorems 3 and 4 offer the security consequences for PI-HDATK.

Theorem 3. Under DBDH assumption, in ROM, $\mathcal{F}$ wins the IND-CCA2 game with a non-negligible advantage ϵ_{datk} when issuing q_{H_i} queries to H_i $(i = 1, 2, 3)$, q_{ke} key extraction queries, q_{gsk} generation symmetric key queries, q_{ke} key encapsulation queries, and q_{kd} key decapsulation queries in a time t, $\mathcal{C}$ resolves DBDH problem with probability

$$\epsilon_{datk} \geq \frac{\epsilon - q_{kd}/2^{k-1}}{2q_{H_1}}$$

within $t' \leq t + O(q_{gsk} + q_{ke} + q_{kd})t_p$, in which t_p is one paring computation.

Proof: Refer to Appendix 3.

Theorem 4. Under BDH assumption, in ROM, $\mathcal{F}$ has a non-negligible advantage $\epsilon_{datk} \geq 10(q_{ke}+1)(q_{ke}+q_{H_3})q_{H_1}/(2^k-1)$ winning the DA-CMA game when issuing q_{H_i} queries to H_i (i = 1, 2, 3), q_{ke} key extraction queries, q_{gsk} generation symmetric key queries, q_{ke} key encapsulation queries, and q_{kd} key decapsulation queries in a time t, $\mathcal{C}$ resolves BDH problem in expected time $t \leq 120686 q_{H_3} q_{H_1} 2^k/\epsilon_{datk}(2^k-1)$.

Proof: Refer to Appendix 4.

7 Performance

We conduct a main computational cost comparison of the construction with existing schemes LZJ [35] and HDA-I of LHO [39] listed in Table 1. The point multiplication in G_1, the exponentiation calculation in G_2, the addition calculations in G_1, and the pairing calculation in G_2 are denoted by PM, EC, AD, and PC, respectively. We ignore XOR, and hash function since they are trivial. In all computational cost, the PC evaluation is the most time-consuming. From Table 1, it shows that the computation overhead of our scheme is less than that of LZJ [35], but more than that of the HDA-I of LHO [39]. It is noted that LZJ [35] is not a heterogeneous DAE scheme which is not catered for the LBS and HDA-I of LHO [39] cannot achieve confidentiality.

An experiment is conducted on the PBC library with A pairing [49]. The A pairing is designed on an elliptic curve $y^2 = x^3 + x \bmod p$ for some prime $p \equiv 3 \bmod 4$. As needed, we set the order of G_1 is q and the library's embedding degree to 2. Here, 80-bit, 112-bit, and 128-bit denotes three kinds of AES [50] key size security level, respectively. Table 2 shows the description for different security levels.

We implement the experiment on an Intel Pentium(R) with 2,048 MB of RAM (2,007.04 MB available) and Dual-Core processor running at 2.69 GHz. On this machine, a PM takes 15.927 ms, and an AD requires 0.065ms employing an ECC with q of 160 bits. A PC and an EC

Table 1. Performance comparison.

Schemes	Computational cost				Security		Heterogeneity
	PM	BP	AD	EP	DA-CMA	IND-CCA2	
LZJ [35]	4	3	1	1	√	√	×
HDA-I of LHO [39]	3	2	1	0	×	√	√
Ours	3	3	0	1	√	√	√

https://doi.org/10.1371/journal.pone.0244978.t001

Table 2. Description for different security level.

Security level	Size of *P*	Size of *q*
80-bit	512	160
112-bit	1024	224
128-bit	1536	256

https://doi.org/10.1371/journal.pone.0244978.t002

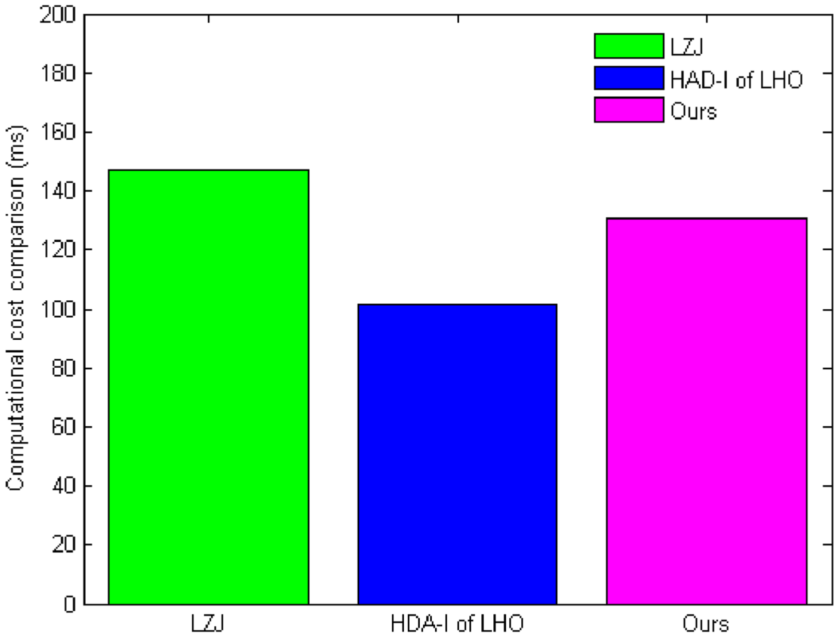


Fig 4. Computational cost comparison.

https://doi.org/10.1371/journal.pone.0244978.g004

take 26.68 ms and 3.126 ms, respectively. LZJ [35] takes 146.939 ms, HDA-I of LHO [39] takes 101.206 ms, and our scheme takes 130.947 ms. Fig 4 depicts the comparative computational cost for LZJ [35], HDA-I of LHO [39], and our scheme. From Fig 4, we can see that the implementation results are consistent with the theoretical analysis.

For the communication cost, LZJ [35], HDA-I of LHO [39], and our scheme are $|m| + |G_1| + |G_2|$. They possess the identical communication cost. $|x|$ is the size of x. For 80-bit security level, $|p| = 512$bits, $|G_1| = 1024$bits, $|q| = 160$bits. If the standard compression techniques are used, G_1 can be reduced to 65bytes. $G_2 = 1024$bits = 128bytes. Therefore, the communication cost of the three schemes is $|m| + |G_1| + |G_2| = |\ m| + 65 + 128 = |m| + 193$bytes. For 112-bit security level, $|p| = 1024$bits, $|G_1| = 2048$bits, $|q| = 224$bits. Using the standard compression technique, G_1 can be reduced to 129bytes. $G_2 = 2048$bits = 256bytes. Therefore, the communication cost of the three schemes is $|m| + |G_1| + |G_2| = |m| + 129 + 256 = |m| + 385$bytes. For 128-bit security level, $|p| = 1536$bits, $|G_1| = 3072$bits, $|q| = 256$bits. Using the standard compression technique, G_1 can be reduced to 193bytes. $G_2 = 3072$bits = 384bytes. Therefore, the communication cost of the three schemes is $|m| + |G_1| + |G_2| = |m| + 193 + 384 = |m| + 577$bytes. Fig 4 shows the communication cost at different security level. It shows that from Fig 5 the 80-bit security level is our best choice for the current computing condition.

8 Application

Zeng et al. [51] presented a deniable ring authentication for protecting the LBS privacy. In their scheme, the user's identity is anonymous to the LBSP and he/she can deny that he/she sends the requested location information to LBSP. However, the entities are all in the same environment and the requested location information is sent in plaintext. Any adversary can monitor or intercept this sensitive information. Therefore, to better resolve this issue, utilize our designed HDAE scheme in LBS systems to render the transmitted message in ciphertext. The specific communication process is as follows:

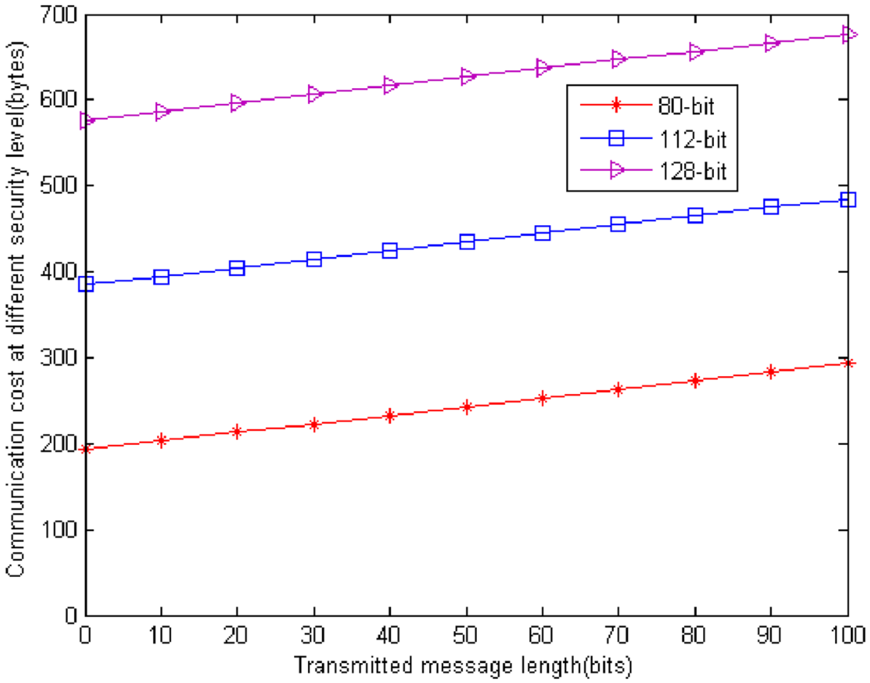


Fig 5. Communication cost at different security level.

https://doi.org/10.1371/journal.pone.0244978.g005

A user in a PKI environment wants to request the location-based service m from the service provider (SP) in an identity-based environment. It first executes the PKI-KG algorithm to produce its private/public key pair (sk_s, pk_s) and executes DAE(m, sk_s, pk_s, ID_r) to create a ciphertext σ. The user then passes the resulting σ to the SP. When the SP receive the LBS request, it first requests a private key S_{ID_r} from the PKG. Then it executes DAD($\sigma, pk_s, ID_r, S_{ID_r}$) to get the LBS request m. It cannot send the response of m to any third party, since the third party cannot ensure whether the LBS request m is from the user or the service provider, due to the fact that the service provider can generate the same LBS request m and ciphertext σ with indistinguishable probabilities.

9 Conclusion

In this paper, we designed a hybrid DAE scheme which comprises a PI-HDAE scheme and a DEM scheme. The entities are in a heterogeneous system where the sender belongs to the PKI environment, while the receiver belongs to the IBC environment. Our construction can achieve confidentiality and deniable authentication in a single logic step. We give a formal security proof in the ROM. Our performance results show that this construction is secure and efficient. Furthermore, we present an example and apply our design to LBS system for better service.

Appendix 1

Proof: Our proof strategy is shown below. The modified games $Game_0$, $Game_1$, $Game_2$ are defined in [52, 53]. The games' difference lies in how the environment replies $\mathcal{F}$'s queries. $\mathcal{F}$ receives the challenge ciphretext $\sigma^* = (\phi^*, c^*)$ that encrypts either m_0 or m_1 by its challenge oracle in the light of b utilizing symmetric key K^*. K^* is also used in the decapsulation ϕ^* with pk_s and ID_r chosen by $\mathcal{F}$. In $Game_i$ (i = 0, 1, 2), it is supposed that S_i is the event $\delta' = \delta$. $\mathcal{F}$'s challenge oracle outputs δ and $\mathcal{F}$ returns δ'. $\mathcal{F}$'s random oracle and $\mathcal{F}$'s oracle determines the probability.

The lemma from [54] is employed as follows.

Lemma 1. Let E, E', and F be events defined on a probability space such that $Pr[E\wedge\neg F] = Pr[E'\wedge\neg F]$. Then, we get $|Pr[E] - Pr[E']| \leq Pr[F]$.

Game$_0$: We execute key extraction algorithm to simulate adversary's view in a real attack. Then we utilize the produced key to reply $\mathcal{F}$'s queries. Thus, the adversary's view is identical to it in a real attack. Hence, we find

$$\left|Pr[S_0] - \frac{1}{2}\right| = \frac{1}{2}Adv_{PI-HDAE}^{IND-CCA2}(\mathcal{F}).$$

Game$_1$: In this game, we only alter how the DAD oracle replies $\mathcal{F}$'s queries. After the calling of the challenge DAE oracle, (ϕ, c), pk_s and ID_r are submitted to the DAD oracle. If $pk_s = pk_s^*$, $ID_r = ID_r^*$, $\phi = \phi^*$, the DAD oracle does not employ the key K, and it utilizes the key K^* to decapsulate c and passes the result to $\mathcal{F}$.

This change does not affect $\mathcal{F}$ and so

$$Pr[S_1] = Pr[S_0].$$

Lemma 2. The running time of a ppt algorithm $\mathcal{C}_1$ is identical to that of $\mathcal{F}$, so we have

$$|Pr[S_2] - Pr[S_1]| = Adv_{PI-HDATK}^{IND-CCA2}(\mathcal{C}_1).$$

Proof: The proof below gives how to design $\mathcal{C}_1$ of the PI-HDATK to be against the IND-CCA2 attack.

The game is between $\mathcal{C}_1$ and $\mathcal{F}$ as follows.

- *Setup*: $\mathcal{C}_1$ passes the *param* to $\mathcal{F}$. Additionally, it also passes the sender's public key pk_s to $\mathcal{F}$.
- *Phase* 1: $\mathcal{F}$ submits a receiver's identity ID_j to $\mathcal{C}_1$. $\mathcal{C}_1$ executes a key extraction (KE) query to its own oracle and transmits the response to $\mathcal{F}$. When $\mathcal{F}$ executes an encryption query on m, and ID_j, $\mathcal{C}_1$ works as follows.

  1. Issue a symmetric key generation (SKG) query on ID_j to gain K.
  2. Calculate $c = DEM.Enc(K, m)$.
  3. Issue a key encapsulation (KES) query on c to gain ϕ.
  4. Return $\sigma = (\phi, c)$.

  When $\mathcal{F}$ executes a key decryption (KD) query on $\sigma = (\phi, c)$, and ID_j, $\mathcal{C}_1$ works as follows.

1. Issue a KD query on (ϕ, c, ID_j) to get K.
2. If $K = \perp$, abort.
3. Calculate $m = DEM.Dec(K, c)$ and output m.

- *Challenge*: $\mathcal{F}$ produces a challenge identity ID_j and messages (m_0, m_1) with equal-lengths. $\mathcal{C}_1$ works as follows.

  1. Pass ID_j to its challenger to gain K_β for $\beta \in \{0, 1\}$.
  2. Elect $\delta \in \{0, 1\}$.
  3. Compute $c^* = DEM.Enc(K_\delta, m_\delta)$.

4. Pass c^* to its challenger to gain ϕ^*.
5. Return $\sigma^* = (\phi^*, c^*)$ to $\mathcal{F}$.

- *Phase* 2: $\mathcal{F}$ issues queries just like in phase 1 except for requesting a KE query on ID_r and a KD query on $\sigma^* = (\phi^*, c^*)$ to gain the corresponding message.
- *Guess*: $\mathcal{F}$ returns δ'. If $\delta' = \delta$, $\mathcal{C}_1$ returns $b' = 1$ which means K_b is a genuine key; or else it returns $b' = 0$ which means K_b is a random key.

When K_b is a genuine key, $\mathcal{F}$ is performed just like it in $Game_1$. It means

$$Pr[S_1] = Pr[\delta' = \delta \mid b = 1] = Pr[b' = 1 \mid b = 1].$$

When K_b is a random key, $\mathcal{F}$ is executed just like it in $Game_2$. It implies

$$Pr[S_1] = Pr[\delta' = \delta \mid b = 0] = Pr[b' = 1 \mid b = 0].$$

Based on PI-HDATK's security definition, we receive

$$Adv_{PI-HDATK}^{IND-CCA2}(\mathcal{C}_1) = |2Pr[b' = b] - 1| = |Pr[b' = 1 \mid b = 1] - Pr[b' = 1 \mid b = 0]|.$$

Lemma 3. The running time of a ppt algorithm $\mathcal{C}_2$ is identical to that of $\mathcal{F}$, so

$$\left|Pr[S_2] - \frac{1}{2}\right| = \frac{1}{2} Adv_{DEM}^{IND-PA}(\mathcal{C}_2).$$

Proof: The proof below gives how to design $\mathcal{C}_2$ of the PI-HDATK to be against the IND-PA attack. $\mathcal{F}$ is run just like the manner in game $Game_2$. Before $\mathcal{F}$ calls its challenge DAE query, we perform the key extraction algorithm to answer $\mathcal{F}$'s query. When $\mathcal{F}$ issues its challenge DAE query on identity ID_r^*, and two messages (m_0, m_1), we just transfer (m_0, m_1) to $\mathcal{C}_2$'s challenge encapsulation oracle to gain c^*. We then issue a GSK query to have K^* and issue a KES query to have ϕ^*. We transmit (ϕ^*, c^*) to $\mathcal{F}$ and drop K^*.

$Pr[S_2]$ is the probability that $\mathcal{C}_2$ pinpoints the challenge encapsulation oracle's hidden bits due to that $\mathcal{C}_2$ returns whatever $\mathcal{F}$ returns.

Appendix 2

Proof: $\mathcal{F}$ attacks the PI-HDAE scheme with advantage $Adv_{PI-HDAE}^{DA-CMA}(\mathcal{F})$. $\mathcal{C}$ attacks DA-CMA for PI-HDATK with advantage at least $Adv_{PI-HDAE}^{DA-CMA}(\mathcal{F})$. We issue $\mathcal{F}$'s queries below.

- *Setup*: $\mathcal{C}$ passes the *param* to $\mathcal{F}$. Additionally, $\mathcal{C}$ also transmits pk_s to $\mathcal{F}$.
- *Attack*: When $\mathcal{F}$ submits an ID_j to $\mathcal{C}$, $\mathcal{C}$ executes a KE query to its own oracles and passes the response to $\mathcal{F}$. When $\mathcal{F}$ performs a DAE query on m, and ID_j, $\mathcal{C}$ issues the SKG query, KES query and KD query just like $\mathcal{C}_1$ works in Lemma 2.
- *Fogery*: $\mathcal{F}$ outputs (m^*, σ^*, ID_r^*), where $\sigma^* = (\phi^*, c^*)$. $\mathcal{C}$ returns (τ^*, ϕ^*, ID_r^*), where $\tau^* = c^*$.

Visibly, this is a perfect proof. If $\mathcal{F}$ wins the DA-CMA game for PI-HDAE, $\mathcal{C}$ has the identical advantage to win the DA-CMA game for PI-HDATK.

Appendix 3

Proof: $\mathcal{C}$ gets an input (P, aP, bP, cP) of DBDH problem and purposes to decide if $\theta = e(P, P)^{abc}$. $\mathcal{C}$ is a challenger and performs $\mathcal{F}$ as a subroutine. $\mathcal{C}$ responds to $\mathcal{F}$'s queries on H_1, H_2 and H_3 and these answers are created randomly. $\mathcal{C}$ reserves lists L_1, L_2 and L_3 to keep the answers. The assumptions are made as follows.

1. Before $\mathcal{F}$ issues KE queries, GSK queries, KES queries and KD queries on identity ID, $\mathcal{F}$ will first inquire H_{ID}.

2. A KES query's encapsulation ciphertext will not be employed in a KD query.

- *Setup*: $\mathcal{C}$ transmits system parameters with $P_{pub} = cP$ to $\mathcal{F}$ in which c is unknown to $\mathcal{C}$. Additionally, $\mathcal{C}$ produces sender's (sk_s, pk_s) and transmits public key pk_s to $\mathcal{F}$.
- *Phase 1*: $\mathcal{F}$ issues queries as follows.
  - H_1 *queries*: $\mathcal{C}$ picks $\gamma \in \{1, 2, \ldots, q_{H_1}\}$. $\mathcal{F}$ requests H_1 queries on its choice identities. At the γ-th query, $\mathcal{C}$ replies by $H_1(ID_\gamma) = bP$. At the j-th query with $j \neq \gamma$, $\mathcal{C}$ picks $w_j \in Z_q^*$, adds (ID_j, w_j) in the list L_1 and responds $H_1(ID_j) = w_j P$.
  - H_2, H_3 *queries*: When $\mathcal{F}$ issues hash value queries, $\mathcal{C}$ checks whether the corresponding items are included in the lists. If yes, $\mathcal{F}$ will get the same answer; otherwise, $\mathcal{F}$ will get a random value. The value and query will be added in the list.
  - *Key extraction queries*: When $\mathcal{F}$ issues key extraction queries on receiver's identity ID_j. If $ID_j = ID_\gamma$, $\mathcal{C}$ aborts. If not, L_1 must comprise (ID_j, w_j) (it implies $\mathcal{C}$ has replied $H_1(ID_j) = w_j P$.) The private key $cH_1(ID_j) = w_j cP = w_j P_{pub}$ is calculated by $\mathcal{C}$ and transmitted to $\mathcal{F}$.
  - *Generation symmetric key queries*: $\mathcal{F}$ submits an ID_j to $\mathcal{C}$. $\mathcal{C}$ then executes $(K, \omega) = Sym(sk_s, pk_s, ID_j)$ and passes K to $\mathcal{F}$. $\mathcal{C}$ saves ω and overwrites the previous value.
  - *Key encapsulation queries*: $\mathcal{F}$ creates τ. $\mathcal{C}$ checks if ω already exists. If not, $\mathcal{C}$ aborts. Or else, $\mathcal{C}$ just executes $\phi = Encap(\omega, \tau)$ and transmits the encapsulation ciphertext ϕ to $\mathcal{F}$.
  - *Key decapsulation queries*: $\mathcal{F}$ sends the receiver's identity ID_j, a tag τ, and an encapsulation ϕ. If $ID_j = ID_\gamma$, (ϕ, τ) is invalid. If $\mathcal{F}$ requests $H_3(t, \tau, pk_s, ID_j)$, where $t = W/e(V, S_{ID_j})$, $\mathcal{C}$ replies h that coincides with $V = hpk_s$, it aborts. From $\mathcal{F}$'s perspective, $\sigma = (W, V)$ is valid. The probability is at most $1/2^k$. If $ID_j \neq ID_\gamma$, $\mathcal{C}$ gains S_{ID_j} by performing the key extraction query. It then passes the result of $Decap(\sigma, \tau, S_{ID_j})$ to $\mathcal{F}$.
- *Challenge*: $\mathcal{F}$ determines when phase 1 is over. It generates a receiver's challenge identity ID_r. If $\mathcal{F}$ has issued a key extraction query on ID_γ, $\mathcal{C}$ aborts. If $\mathcal{F}$ does not pick $ID_r = ID_\gamma$ as the target identity, it aborts too. $\mathcal{C}$ picks $W^* \in G_2$, sets $V^* = aP$ and computes $t^* = W^*/\theta$ (θ is DBDH problem's candidate). Then $\mathcal{C}$ issues H_2 query to look for $K_1 = H_2(t^*)$. $\mathcal{C}$ randomly picks $K_0, \beta \in (0, 1)$, and passes K_β to $\mathcal{F}$. $\mathcal{F}$ then passes τ^* to $\mathcal{C}$. Whereafter, $\mathcal{C}$ transmits $\sigma^* = (W^*, V^*)$ to $\mathcal{F}$.
- *Phase 2*: $\mathcal{F}$ issues queries as in phase 1 except that it has no ability to issue a KE query on ID_r and a KD query on (ϕ^*, τ^*) to gain the symmetric key.
- *Guess*: $\mathcal{F}$ outputs β' for $(K_\beta, \omega^*) = Sym(sk_s, pk_s, ID_r)$ and $\phi^* = Encap(\omega^*, \tau^*)$ hold. If $\beta' = \beta$, $\mathcal{C}$ outputs 1 shows $\theta = e(P, P)^{abc}$; If not, $\mathcal{C}$ outputs 0 shows $\theta \neq e(P, P)^{abc}$.

Now we calculate $\mathcal{C}$'s successful probability. If one of the events below is satisfied, $\mathcal{C}$ will fail:

- E_1 $\mathcal{F}$ does not pick ID_γ as the receiver's identity in challenge phase.
- E_2 $\mathcal{F}$ has issued a KE query on ID_γ.
- E_3 $\mathcal{C}$ terminates in a KD query due to it refuses a valid encapsulation.

We show that $\Pr[\neg E_1] = 1/q_{H_1}$, and $\Pr[E_3] \leq q_{kd}/2^k$. Additionally, $\neg E_1$ means $\neg E_2$.
Because
$p_1 = \Pr[\beta' = \beta|(K_\beta, \omega^*) = \mathrm{Sym}(pk_s, sk_s, ID_r)]$ and $\phi* = Encap(\omega*, \tau*) = \frac{\epsilon+1}{2} - \frac{q_{kd}}{2^k}$

and
$p_0 = \Pr[\beta' = i | \theta \in_R G_2] = \frac{1}{2}$ for $i = 0, 1$,
We get

$$\mathrm{Adv}(\mathcal{C}) = \frac{|p_1 - p_0|}{q_{H_1}} = (\frac{\epsilon + 1}{2} - \frac{q_{kd}}{2^k} - \frac{1}{2})(\frac{1}{q_{H_1}}) = \frac{\epsilon - q_{kd}/2^{k-1}}{2q_{H_1}}$$

$O(q_{gsk} + q_{ke} + q_{kd})$ is $\mathcal{C}$'s computation time that shows pairing computations in GSK queries, KE queries and KD queries.

Appendix 4

Proof: we have to let our design fit into the signature scheme described in [54], where the simulation step can be simulated in the absence of the sender's private key (i.e., absence of the master private key). On this occasion, we need an approach to resolve the BDH problem.

First, we observe that the PI-HDATK scheme accords with the requested three-phase honest-verifier zero-knowledge identification protocol, where $\sigma_1 = t$ is the commitment, $h = H_3(\tau, t, pk_s, ID_r)$ is the hash value, and $\sigma_2 = W$ is the answer.

Second, a simulation step is shown and an approach of how to resolve the BDH problem is given. Given (P, aP, bP, cP) of BDH problem, $\mathcal{C}$ needs to compute $h = e(P, P)^{abc}$. $\mathcal{C}$ performs $\mathcal{F}$ as a subroutine. $\mathcal{F}$ consults $\mathcal{C}$ to reply H_1, H_2, and H_3 and $\mathcal{C}$ holds L_1, L_2, and L_3 to preserve the resulting responses. The process below is depicted.

- *Setup*: $\mathcal{C}$ calculates params with $P_{pub} = cP$ and passes them to $\mathcal{F}$. Additionally, $\mathcal{C}$ also transmits $pk_s = aP$ to $\mathcal{F}$.
- *Attack*: $\mathcal{F}$ executes the following queries.
  - H_1 *queries* $\mathcal{C}$ picks $\gamma \in \{1, 2, \ldots, q_{H_1}\}$. $\mathcal{F}$ requests H_1 queries on its choice identities. At the γ-th query, $\mathcal{C}$ replies by $H_1(ID_\gamma) = bP$. At the j-th query with $j \neq \gamma$, $\mathcal{C}$ picks $w_j \in Z_q^*$, inserts (ID_j, w_j) in the list L_1 and responds $H_1(ID_j) = w_j P$.
  - H_2, H_3 queries, KE queries, GSK queries, KES queries, and KD queries are identical to them in Theorem 3.
- *Fogery*: $\mathcal{F}$ outputs a triple $(\sigma^*, \tau^*, ID_\gamma)$, where $\sigma^* = (W^*, V^*)$. We coalesce ID_γ and τ^* into a "generalized" forged tag (ID_γ, τ^*) to hide the identity-based aspect of the DA-CMA attack, and simulate the setting of an identity-less adaptive-CMA existential forgery. If $\mathcal{F}$ is an efficient forger, then we have the capability to constitute a Las Vegas machine $\mathcal{F}'$ that outputs $((ID_\gamma, \tau^*), h^*, \sigma^*)$ and $((ID_\gamma, \tau^*), \bar{h}^*, \bar{\sigma}^*)$ with $h^* \neq \bar{h}^*$ and the same commitment t^*. To resolve the BDH problem based on the machine $\mathcal{F}'$, we constitute a machine $\mathcal{C}'$ as follows.

1. $\mathcal{C}'$ performs $\mathcal{F}'$ to gain two distinct signatures $((ID_\gamma, \tau^*), h^*, \sigma^*)$ and $((ID_\gamma, \tau^*), \bar{h}^*, \bar{\sigma}^*)$.
2. $\mathcal{C}'$ computes $e(P, P)^{abc}$ as $(W^*/\bar{W}^*)^{1/(h^* - \bar{h}^*)}$.

From the forking lemma [54] and the lemma on relationship between given-identity and chosen-identity attack [55], if $\mathcal{F}$ succeeds with probability $\epsilon_{datk} \geq 10(q_{ke} + 1)(q_{ke} + q_{H_3})q_{H_1}/(2^k - 1))$ in time t, then $\mathcal{C}'$ resolves the BDH problem in expected time $t \leq 120686 q_{H_3} q_{H_1} 2^k/\epsilon_{datk}(2^k - 1)$.

Supporting information

S1 File.
(DOCX)

Acknowledgments

The authors thank the anonymous reviewers and the Editor for the constructive comments and generous feedback.

Author Contributions

Conceptualization: Guanhua Chen.

Formal analysis: Ge Kan, Chengjie Xu.

Investigation: Changhui Yu.

Methodology: Chunhua Jin.

Validation: Ying Jin.

References

1. Sun G, Chang V, Ramachandran M, Sun Z, Li G, Yu H, et al. Efficient location privacy algorithm for Internet of Things (IoT) services and applications. Journal of Network and Computer Applications. 2017; 89: 3–13. https://doi.org/10.1016/j.jnca.2016.10.011
2. Peng T, Liu Q, Meng D, Wang G. Collaborative trajectory privacy preserving scheme in location-based services. Information Sciences. 2017; 387: 165–179. https://doi.org/10.1016/j.ins.2016.08.010
3. Yoon S, Kim J, Connolly DJ. Understanding motivations and acceptance of location-based services. International Journal of Hospitality & Tourism Administration. 2018; 19(2): 187–209. https://doi.org/10.1080/15256480.2017.1305316
4. Zhang S, Wang G, Bhuiyan MA, Liu Q. A dual privacy preserving scheme in continuous location-based services. IEEE Internet of Things Journal. 2018; 5(5): 4191–4200. https://doi.org/10.1109/JIOT.2018.2842470
5. Ma C, Yan Z, Chen CW. SSPA-LBS: Scalable And Social-Friendly Privacy-Aware Location-Based Services. IEEE Transactions on Multimedia. 2019; 21(8): 2146–2156. https://doi.org/10.1109/TMM.2019.2892300
6. Ataei M, Degbelo A, Kray C, Santos V. Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services. ISPRS international journal of geo-information. 2018; 7(11). https://doi.org/10.3390/ijgi7110442
7. Memon I, Hussain I, Akhtar R, Chen G. Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme. Wireless Personal Communications. 2015; 84(2): 1487–1508. https://doi.org/10.1007/s11277-015-2699-1
8. Xie Q, Wang L. Privacy-Preserving Location-Based Service Scheme for Mobile Sensing Data. Sensors. 2016; 16: 1993. https://doi.org/10.3390/s16121993 PMID: 27897984
9. Sun G, Liao D, Li H, Chang V. L2P2: A location-label based approach for privacy preserving in LBS. Future Generation Computer Systems. 2017; 375–384. https://doi.org/10.1016/j.future.2016.08.023
10. Asuquo P, Cruickshank H, Morley J, Ogah CP, Lei A, Hathal W, et al. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet of Things Journal. 2018; 5(6): 4778–4802. https://doi.org/10.1109/JIOT.2018.2820039
11. Zhang Y, Xu C, Li H, Yang K, Zhou J, Lin X. HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems. IEEE Transactions on Industrial Informatics. 2018; 14(9): 4101–4112. https://doi.org/10.1109/TII.2018.2832251
12. Zhou J, Cao Z, Qin Z, Dong X, Ren K. LPPA: Lightweight Privacy-preserving Authentication from Efficient Multi-key Secure Outsourced Computation for Location-based Services in VANETs. IEEE Transactions on Information Forensics and Security. 2020; 420–434. https://doi.org/10.1109/TIFS.2019.2923156

13. Zhu X, Ayday E, Vitenberg R. A privacy-preserving framework for outsourcing location-based services to the cloud. IEEE Transactions on Dependable and Secure Computing. 2019; 1–1. https://doi.org/10.1109/TDSC.2019.2892150

14. Wang H, Zhang Z, Taleb T. Special issue on security and privacy of IoT. World Wide Web. 2018; 21(1): 1–6. https://doi.org/10.1007/s11280-017-0490-9

15. Wang H, Wang Y, Taleb T, Jiang X. Special issue on security and privacy in network computing. World Wide Web. 2020; 23(2): 951–957. https://doi.org/10.1007/s11280-019-00704-x

16. Zhang F, Wang Y, Liu S, Wang H. Decision-based evasion attacks on tree ensemble classifiers. World Wide Web. 2020; 1–21.

17. Aumann Y, Rabin M. Authentication, enhanced security and error correcting codes. Proc. Cryptology—CRYPTO'98, 1998; 299–303.

18. Wu W, Li F. An Efficient Identity-Based Deniable Authenticated Encryption Scheme. Ksii Transactions on Internet and Information Systems. 2015; 9(5): 1904–1919.

19. Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing. 2003; 33(1): 167–226. https://doi.org/10.1137/S0097539702403773

20. Abe M, Gennaro R, Kurosawa K. Tag-KEM/DEM: A new framework for hybrid encryption. Journal of Cryptology. 2008; 21(1): 97–130. https://doi.org/10.1007/s00145-007-9010-x

21. Choi KY, Cho J, Hwang JY, Kwon T. Constructing efficient PAKE protocols from identity-based KEM/DEM. Proc. Information Security Applications—16th International Workshop, WISA 2015. 2015; 411–422.

22. Emura K, Kanaoka A, Ohta S, Takahashi T. A KEM/DEM-based construction for secure and anonymous communication. Proc. 39th IEEE Annual Computer Software and Applications Conference, COMPSAC 2015. 2015; 2: 1–5.

23. Xu J, Wen Q, Li W, Jin Z. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. IEEE transactions on parallel and distributed systems. 2015; 27(1):119–129. https://doi.org/10.1109/TPDS.2015.2392752

24. Bansal TK, Chang D, Sanadhya SK. Sponge based CCA2 secure asymmetric encryption for arbitrary length message. Proc. Information Security and Privacy—20th Australasian Conference, ACISP 2015. 2015; 93–106.

25. Ishida Y, Shikata J, Watanabe Y. CCA-secure revocable identity-based encryption schemes with decryption key exposure resistance. International Journal of Applied Cryptography. 2017; 3(3): 288–311. https://doi.org/10.1504/IJACT.2017.086229

26. Wu X, Han Y, Zhang M, Zhu S. Parallel Long Messages Encryption Scheme Based on Certificateless Cryptosystem for Big Data. Proc. Information Security and Cryptology-13th International Conference, Inscrypt 2017. 2017; 211–222.

27. Giacon F, Kiltz E, Poettering B. Hybrid encryption in a multi-user setting, revisited. Proc. Public-Key Cryptography—PKC 2018—21st IACR International Conference on Practice and Theory of Public-Key Cryptography. 2018; 159–189.

28. Ge A, Wei P. Identity-based broadcast encryption with efficient revocation. Proc. Public-Key Cryptography—PKC 2019—22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. 2019; 405–435.

29. Sakai Y, Hanaoka G. A Remark on an Identity-Based Encryption Scheme with Non-interactive Opening. Proc. 2018 International Symposium on Information Theory and its Applications (ISITA). 2018; 703–706.

30. Baek J, Susilo W, Salah K. Ha JS, Damiani E, You I. Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment. Proc. Cyber Security: Principles, Techniques, and Applications. 2019; 1–22.

31. Li F, Zhong D, Takagi T. Efficient deniably authenticated encryption and its application to e-mail. IEEE Transactions on Information Forensics and Security. 2016; 11(11): 2477–2486. https://doi.org/10.1109/TIFS.2016.2585086

32. Jin C, Chen G, Yu C, Zhao JY. Deniable authenticated encryption for e-mail applications. International Journal of Computers and Applications. 2018; 1–10.

33. Rasmussen K, Gasti P. Weak and Strong Deniable Authenticated Encryption: On their Relationship and Applications. Proc. 16th Annual Conference on Privacy, Security and Trust, PST 2018. 2018; 1–10.

34. Huang W, Liao Y, Zhou S, Chen H. An Efficient Deniable Authenticated Encryption Scheme for Privacy Protection. IEEE Access. 2019; 7:43453–43461. https://doi.org/10.1109/ACCESS.2019.2907250

35. Li F, Zheng Z, Jin C. Identity-based deniable authenticated encryption and its application to e-mail system. Telecommunication Systems. 2016; 62(4): 625–639. https://doi.org/10.1007/s11235-015-0099-1

36. Jin C, Zhao J. Efficient and short identity-based deniable authenticated encryption. Proc. Cloud Computing and Security—Third International Conference, ICCCS 2017. 2017; 244–255.

37. Ahene E, Jin C, Li F. Certificateless deniably authenticated encryption and its application to e-voting system. Telecommunication Systems. 2019; 70(3): 417–43. https://doi.org/10.1007/s11235-018-0496-3

38. Chen G, Zhao J, Jin Y, Zhu Q, Jin C, Shan J, et al. Certificateless Deniable Authenticated Encryption for Location-Based Privacy Protection. IEEE Access. 2019; 7: 101704–101717. https://doi.org/10.1109/ACCESS.2019.2931056

39. Li F, Hong J, Omala AA. Practical deniable authentication for pervasive computing environment. Wireless Networks. 2018; 24(1): 139–149. https://doi.org/10.1007/s11276-016-1317-9

40. Jin C, Chen G, Yu C, Zhao J, Jin Y, Shan J. Heterogeneous deniable authentication and its application to e-voting systems. Journal of information security applications. 2019; 47: 104–111. https://doi.org/10.1016/j.jisa.2019.04.009

41. An JH, Dodis Y, Rabin T. On the security of joint signature and encryption. Proc. Cryptology—EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques. 2002; 83–107.

42. Boneh D, Franklin M. Identity-based encryption from the weil pairing. SIAM Journal on Computing. 2003; 32(3): 586–615. https://doi.org/10.1137/S0097539701398521

43. Zhang Y, Xu C, Lin X, Shen XS. Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. IEEE Transactions on Cloud Computing. 2019; 1–1. https://doi.org/10.1109/TCC.2019.2908400

44. Miao Y, Liu X, Choo KR, Deng RH, Li J, Li H, et al. Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. IEEE Transactions on Dependable and Secure Computing. 2019; 1–1.

45. Zhang X, Wang H, Xu C. Identity-based key-exposure resilient cloud storage public auditing scheme from lattices. Information Sciences. 2019; 472: 223–234. https://doi.org/10.1016/j.ins.2018.09.013

46. Kabir E, Mahmood A, Wang H, Mustafa AK. Microaggregation sorting framework for k-anonymity statistical disclosure control in cloud computing. IEEE Transactions on Cloud Computing, 2015; 1–1.

47. Wang Y, Shen Y, Wang H, Cao J, Jiang X. Mtmr: Ensuring mapreduce computation integrity with merkle tree-based verifications. IEEE Transactions on Big Data. 2016; 4(3): 418–431. https://doi.org/10.1109/TBDATA.2016.2599928

48. Cheng K, Wang L, Shen Y, Wang H, Wang Y, Jiang X, et al. Secure k-nn query on encrypted cloud data with multiple keys. IEEE Transactions on Big Data. 2017; 1–1. https://doi.org/10.1109/TBDATA.2017.2707552

49. PBC Library. http://crypto.stanford.edu/pbc/.

50. Daemen J, Rijmen V. The design of Rijndael: AES-The Advanced Encryption Standard. Springer Science & Business Media. 2013.

51. Zeng S, Tan S, Chen Y, He M, Xia M, Li X. Privacy-preserving location-based service based on deniable authentication. Proc. 9th International Conference on Utility and Cloud Computing (UCC). 2016; 276–281.

52. Zhang Y, Xu C, Ni J, Li H, Shen X. Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storag. IEEE Transactions on Cloud Computing. 2019; 1–1. https://doi.org/10.1109/TCC.2019.2908400

53. Zhang Y, Xu C, Liang X, Li H, Mu Y, Zhang X. Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation. IEEE Transactions on Information Forensics and Security. 2016; 12(3): 676–688. https://doi.org/10.1109/TIFS.2016.2631951

54. Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology. 2000; 13(3): 361–396. https://doi.org/10.1007/s001450010003

55. Cha JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. Proc. Public Key Cryptography—PKC 2003. 2003; 18–30.