Journal of Ambient Intelligence and Humanized Computing (2018) 9:1889–1899
https://doi.org/10.1007/s12652-017-0672-4

ORIGINAL RESEARCH

Accountable mobile E-commerce scheme in intelligent cloud system transactions

Mingwu Zhang[1] · Yao Yao[1] · Yan Jiang[1] · Bingbing Li[1] · Chunming Tang[2]

Received: 12 September 2017 / Accepted: 28 December 2017 / Published online: 1 February 2018

Abstract
The vivid and rapid development of the Internet motivates cloud-based intelligent information systems to be applied. Mobile e-commerce, as a new business model based on cloud computing in intelligent service, has become the mainstream of mobile applications. It not only provides efficient computation services for both trading parties, but also gives a secure and reliable data storage center. However, privacy and accountability have become one of users' crucial concerns in mobile e-commerce transactions. In this paper, we present a practical and efficient accountable mobile e-commerce scheme that is based on cloud platform to address the fundamental transaction requirement. We propose the concrete construction and demonstrate that the proposed scheme can provide effective security in the transaction process, and also give the practical deployment in cloud computing systems to provide the intelligent information services. We also give the performance analysis and show it is efficient and practical compared with related methods in terms of computation complexity and communication costs.

Keywords Plaintext checkability · Mobile E-commerce · Accountability · Intelligent cloud · Encryption with equality test

1 Introduction

1.1 Background

Nowadays, cloud computing has become one of hottest focuses in academia, enterprise and even the government, which provides a dynamic, scalable, virtualized computing model over the Internet for intelligent information services. It is also through network to obtain the necessary resources, which contains core content of one is to achieve resource scheduling and management, and the other is to provide services on-demand (Buyya et al. 2008; Shen et al. 2017). Cloud computing grows fast and has quite extensive application fields (for example, the e-commerce). E-commerce, as a new type of transaction, brings enterprise, logistic and consumer into a comprehensive network economy era. Consumers can expediently complete a variety of complex e-commerce activities, such as bank account withdrawal, transaction information inquiry and commodity trading service. In traditional transaction mode, dramatic increase of server traffic within a certain period of time will inevitably lead to server paralysis. However, with the support of cloud computing services, e-commerce platform can effectively cope with the rapid increase of traffic, thus provide users with good quality of service (Yang and Liu 2010).

Traditional e-commerce system relies on fixed location like the workstations or desktops (Yang and Zheng 2012), which is the limitation of e-commerce. The rise of intelligent terminal device has promoted the renewal of modern business model. With the widespread use of 4G mobile network (Varshney and Jain 2001; Han and Choi 2013; Hwang et al. 2015; Shen et al. 2016) and Wi-Fi (Duarte et al. 2012; Kim et al. 2015; Torres-Sospedra et al. 2015; Brown et al. 2012; Zhu and Yang 2015; Zhang and Mu 2016), mobile e-commerce takes advantage of wireless terminal such as mobile phone, PAD, notebook for e-commerce activities (Seo and Emura 2014), enabling users to access the Internet and conduct transactions anytime and anywhere. In terms of user scale, mobile e-commerce will gradually replace the traditional e-commerce sooner or later. A typical interaction

✉ Mingwu Zhang
mzhang@mail.hbut.edu.cn

Chunming Tang
ctang@gzhu.edu.cn

[1] School of Computers, Hubei University of Technology, Wuhan, China

[2] School of Mathematics and Information Science, Guangzhou University, Guangzhou, China

mode between mobile client and cloud server is illustrated in Fig. 1.

The interaction between intelligent mobile client and cloud data center can be performed on the Internet. Cloud computing deploys the business resources in the data center, providing a series of services to users. In this way, it is not only to reduce the operation load of terminal, improve the efficiency of the cloud data center, but also provides efficient computing services for both parties. The payment service is the most important link in the whole transaction, and the mobile payment is widely used recently (Ye and Xiao 2013). The mobile payments bind mobile terminal to bank card, and the users can conduct transaction anytime and anywhere only with mobile phone. Also, the third-party payment has become the most popular usage mode in its industrial structure. When the users require to make a payment, the payment service in data center will issue a transaction application to third-party payment, which will return payment result to the users.

1.2 Related work

Even though intelligent mobile e-commerce on the cloud computing has enough advantages, it still exists some new security and privacy concerns (Ghosh and Swaminatha 2001; Tang and Wu 2008; Jo et al. 2014; Biswas and Vidyasankar 2014; Fu et al. 2016; Xia et al. 2015; Kolodziej and Xhafa 2011) that greatly influence user's reliance. If we order a service or personal belongings which are private and unwilling to be seen by other users beyond the vendor. Our order record needs to be encrypted. On the other hand, there might also be a consideration that a dishonest user (buyer or vendor) could lead to transaction failure. For example, we often encounter the situation that vendor provides wrong goods or service unintentional, resulting in dispute. Hence, how to protect users' privacy and resolve dispute is a problem. Han et al. (2016) proposed a mobile e-commerce scheme to combine identity-based plaintext-checkable encryption (IBPCE) with IBS. However, Han et al.'s scheme is inefficient. To improve the efficiency of Han et al., we propose a new IBPCE scheme instead of Paterson et al. IBS scheme (Paterson and Schuldt 2006). The initial idea of identity-based encryption system was proposed by Shamir (1984) in order not to using the public-key certificates. It is defined as a special type of public-key encryption where an user's public key may be arbitrary string that has its own meaning to an user's identity, such as a telephone number or an e-mail address. Boneh and Franklin (2001) first designed a secure and truly practical IBE system using bilinear maps and proved its security in the random oracle model. Subsequently, plenty of work (Park and Lee 2016; Wang 2007; Waters 2005; Ma 2016; Seo and Emura 2014; Gentry 2006) has been devoted to constructing pairing-based IBE systems and are provable secure in the different models. Among the previous IBE systems, Waters (2005) and Gentry (2006) proposed two efficient and practical IBE schemes which are fully secure in the standard model, respectively. In traditional public-key encryption scheme, checking whether a ciphertext is the encryption of a plaintext under the public key is difficult when the secret key is unknown. To solve this problem, Canard et al. (2012) proposed and studied a new cryptographic primitive called plaintext-checkable encryption with additional functionality that anyone can test whether a ciphertext is the encryption of a given plaintext under the public key. For instance, a dishonest sender who does not know the receiver's secret key can be identified if he sends an incorrect ciphertext to the receiver. Therefore, a PCE scheme can provide not only confidentiality but also accountability Han et al. (2016). The concept of Identity-based Plaintext-checkable Encryption (IBPCE) was first proposed by Han et al. (2016) in 2016, which is derived from Gentry's IBE scheme (Gentry 2006) and Canard et al.'s PCE scheme (Canard et al. 2012), whose security is proved in the standard model.

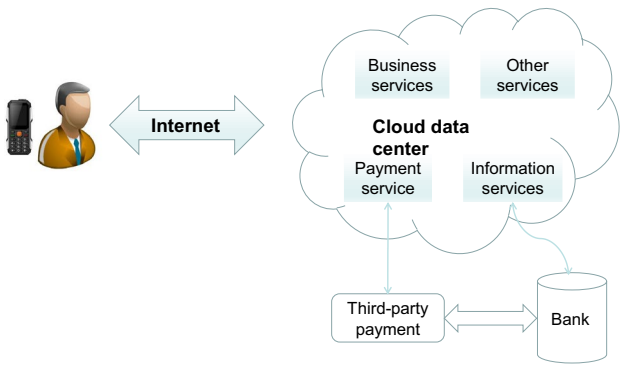

Fig. 1 Interaction between mobile client and intelligent cloud server

1.3 Our Contribution

We first propose an IBPCE scheme combined with Paterson's IBS scheme (Paterson and Schuldt 2006), which can be applied to E-commerce scenario and result in an accountable mobile e-commerce (AMEC) transaction. Our contribution is described as follows:

1. We propose a new IBPCE scheme for mobile e-commerce using bilinear pairing, and prove it to be secure based on the decisional q-ABDHE assumption in the standard mode. Besides, compared with related IBPCE scheme, our scheme can better meet the efficiency requirement of mobile transaction by reducing computation costs and improving communication efficiency.

2. We combine our IBPCE scheme with identity-based signature and incorporate into the mobile transaction scenario to present a new AMEC scheme based on cloud computing environments. In this scheme, the transactions between buyer and vendor are encrypted. Meanwhile, an offline adjudicator will be added in case of dispute between buyer and vendor. It is worth mentioning that the IBS scheme we use is derived from the Paterson et al.'s IBS scheme which is combined with Han et al's IBPCE scheme. The former is proved to be more secure and efficient. Therefore, our incorporative AMEC scheme has a greater improvement compared with Han et al's.
3. Finally, we give the user interaction process protocol, and analyze the results of the mobile e-commerce system in cloud computing environment, and also provide the protocol performance in theoretical analysis and simulated benchmark experiment.

1.4 Organization

The rest of this paper is organized as follows. The preliminaries which are used throughout this paper are presented in Sect. 2. In Sect. 3, we give the proposed IBPCE scheme, followed by its security analysis and comparison with related schemes. In Sect. 4, the proposed IBPCE scheme is applied in mobile e-commerce scenario which results in an accountable mobile e-commerce scheme. We give details of its performance evaluation in Sect. 5. Finally, Sect. 6 concludes this paper.

2 Preliminaries

In this section, we briefly review some preliminaries such as bilinear maps, complexity assumptions, formal definition and security model of IBPCE, and the IBS framework, respectively.

Let $p \in \mathcal{Z}^+$, we denote $\mathcal{Z}_p$ by $\{1, 2, \ldots, p-1\}$. A function is *negligible* in parameter λ (denoted $\epsilon(\lambda)$) if it is smaller than the inverse of any polynomial, for all large enough value of λ. We use the notation $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ to denote an adversary, a simulator and a challenger in our system.

2.1 Bilinear group and complexity assumption

We first review bilinear maps, using the following standard notation Let $\mathbb{G}$ and $\mathbb{G}_\tau$ are two multiplicative cyclic groups with prime order p, and g is a generator of $\mathbb{G}$.

A function map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$ is called a *bilinear map* which satisfies the following three properties: (1)*Bilinearity*: for $\forall g \in \mathbb{G}$ and $a, b \in \mathcal{Z}_p$, the equality $e(g^a, g^b) = e(g, g)^{ab}$ holds; (2)*Non-degeneracy*: in the sense that $e(g, g) \neq 1$ for any $g \in \mathbb{G}$; (3)*Computability*: For $\forall g \in G$, there exists an efficient algorithm to evaluate $e(g, g)$.

We say that $\mathbb{G}$ and $\mathbb{G}_\tau$ are bilinear groups if the group operations in $\mathbb{G}$ and $\mathbb{G}_\tau$ as well as the bilinear map e above are all efficiently computable. Namely, the bilinear groups can be efficiently constructed by Weil pairing or Tate pairing.

The security of our scheme is based on a complexity assumption that called the decisional q-augmented bilinear Diffie-Hellman exponent (decisional q-ABDHE) assumption (Gentry 2006), where q is (roughly) the anticipated number of private key generation queries.

Definition 1 (*q-ABDHE assumption*) Let bilinear group generating $\mathcal{G}(1^\lambda) \to (\mathbb{G}, \mathbb{G}_\tau, e, p)$ and g, g' be generators of $\mathbb{G}$. The decisional q-ABDHE problem: Given a vector of elements in group $\mathbb{G}$, i.e.,

$$(g', g'^{\alpha^{q+2}}, g, g^\alpha, g^{\alpha^2}, \ldots, g^{\alpha^q}, g^{\alpha^{q+2}}, \ldots, g^{\alpha^{2q}}) \in \mathbb{G}^{2q+2}$$

as input, and to decide whether $R = e(g, g')^{\alpha^{q+1}}$ or not is hard.

2.2 Formal definition and security model

Definition 2 (*Identity-based Plaintext-checkable Encryption, IBPCE*) An IBPCE scheme consists of five algorithms: IBPCE= (Setup, Extract, Encrypt, Decrypt, Check), whose functionalities are described as:

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, \mathsf{msk})$: taking a security parameter λ as input, the algorithm returns the public parameters pp and a master private key msk.
- $\mathsf{Extract}(\mathsf{msk}, \mathsf{pp}, \mathsf{id}) \to \mathsf{pdk}_{\mathsf{id}}$: using the master key msk and an identity id, the algorithm returns a private decryption key for identity id.
- $\mathsf{Encrypt}(\mathsf{pp}, \mathsf{id}, M) \to \mathsf{ct}$: taking an identity id, the public parameter pp and a plaintext M as inputs, the algorithm returns the corresponding ciphertext ct.
- $\mathsf{Decrypt}(\mathsf{ct}, \mathsf{pdk}_{\mathsf{id}}) \to M$: using a private decryption key $\mathsf{pdk}_{\mathsf{id}}$ to decrypt ciphertext ct, the algorithm returns the corresponding plaintext M.
- $\mathsf{Check}(\mathsf{pp}, \mathsf{ct}, \mathsf{id}, M) \to 1/0$: taking an identity id, a ciphertext ct and a plaintext M as inputs, the algorithm returns 1 if ciphertext ct is the encryption of plaintext M under the identity id. Otherwise, it returns 0.

The security model of IBPCE scheme is similar to that in (Canard et al. 2012). It is defined by the following game executed between a challenger $\mathcal{C}$ and an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, where $\mathcal{A}_1$ and $\mathcal{A}_2$ represent the find and guess stage, respectively. It is assumed that $\mathcal{A}_1$ and $\mathcal{A}_2$ share neither coin nor state.

1. Setup: The challenger $\mathcal{C}$ runs Setup algorithm, and sends the public parameter pp to adversary $\mathcal{A}$.
2. Phase1: $\mathcal{A}_1$ can adaptively query the key generation oracle with an identity id. The challenger $\mathcal{C}$ runs Extract algorithm on id and forwards the resulting private decryption key $\mathsf{pdk}_{\mathsf{id}}$ to the adversary $\mathcal{A}_1$. This query can be performed multiple times.
3. Challenge: $\mathcal{A}_1$ submits a challenge identity id' and two plaintexts (M_0, M_1) with the same length. Note that id' must not have appeared in any key generation query of phase 1. The challenger $\mathcal{C}$ flips an unbiased coin with $\{0, 1\}$, and obtains a bit b. Then, challenger $\mathcal{C}$ sets $\mathsf{Encrypt}(\mathsf{pp}, \mathsf{id}, M_b) \rightarrow \mathsf{ct}'$, and sends ct' to adversary $\mathcal{A}_1$ as its challenge ciphertext.
4. Phase2: This is identical to Phase 1, with the restriction that the adversary $\mathcal{A}_2$ cannot request a private decryption key for id'.
5. Guess: $\mathcal{A}_2$ submits his guess b'. In the experiment the adversary $\mathcal{A}$ wins if $b' = b$.

Definition 3 An IBPCE scheme is (t, q, ϵ)-IND-ID-CPA secure if any probabilistic polynomial-time adversary making at most q-times secret key queries with the advantage at most ϵ in winning the above game

$$Adv^{\mathsf{ID-CPA}}_{\mathsf{IBPCE},\mathcal{A}}(\lambda) = \left| \Pr[b' = b] - 1/2 \right| \leq \epsilon(\lambda) \tag{1}$$

where the advantage is taken over the random bits used by the challenger and the adversary, and $\epsilon(\lambda)$ is a negligible function in λ.

2.3 IBS framework

An identity-based signature (IBS) is a digital signature that can provide non-repudiation and integrity in the identity setting. An IBS scheme can be described as four algorithms:

- $\mathsf{IBS.Setup}(1^\lambda) \rightarrow (\mathsf{pp}, \mathsf{msk})$: It takes as input security parameter λ, and the PKG generates public system parameter pp and a master secret key msk.
- $\mathsf{IBS.Extract}(\mathsf{pp}, \mathsf{msk}, \mathsf{id})$: It takes as input public system parameter pp, the master secret key *msk* and an identity id, and generates a signing key $\mathsf{sk}_{\mathsf{id}}$.
- $\mathsf{IBS.Sign}(\mathsf{pp}, M, \mathsf{sk}_{\mathsf{id}})$: It takes as input public system parameter pp, a plaintext M and a signing key $\mathsf{sk}_{\mathsf{id}}$, and generates a signature σ_M on the plaintext M.
- $\mathsf{IBS.Verify}(\mathsf{pp}, M, \mathsf{id}, \sigma_M)$: It takes as input public system parameter pp, a plaintext M, an identity id and a signature σ_M, and outputs 1 (accept) if is a valid signature on the plaintext M. Otherwise, it outputs 0 (reject).

2.4 System model and roles

Figure 2 shows the system model of our scheme, with four roles described as follows:

Key generation center (KGC) is responsible for setting up system, generating the public system parameter pp and the master private key msk. Meanwhile, it creates private decryption key $\mathsf{pdk}_{\mathsf{id}}$ and sends $user_{\mathsf{id}}$ to via a secure channel.

Buyer must register to obtain the private decryption key $\mathsf{pdk}_{\mathsf{id}}$. If the buyer wants to order service or personal belongings from vendor. He encrypts his order M_B and generates signature σ_{HB} and sends them to the cloud data server. Note that only the vendor could verifies signature σ_{HB} and decrypt the encrypted order information.

Vendor must register to obtain the private decryption key $\mathsf{pdk}_{\mathsf{id}}$. Additionally, the vendor can verify signature σ_{HB} and uses $\mathsf{pdk}_{\mathsf{id}}$ to decrypt buyer's encrypted order information that stored in the cloud data server. Then, the vendor encrypts the service or personal belongings M_V required by the buyer and generates signature σ_{HV} and sends them to the buyer.

Cloud data server is in charge of resolving possible dispute between registered buyer and vendor, and returning the identification results. In addition, the buyer and vendor need to submit $(M_B, M_V, \mathsf{id}_B, \mathsf{ct}_B, \sigma_{HB})$ and $(M_B, M_V, \mathsf{id}_V, \mathsf{ct}_V, \sigma_{HB})$ to cloud data server, respectively, so that the server can check the encrypted transaction records to identify who is dishonest and return a feedback.

3 Proposed scheme

In this section, we give the proposed identity-based plaintext-checkable encryption (IBPCE) scheme, and prove its security and finally provide the performance analysis.

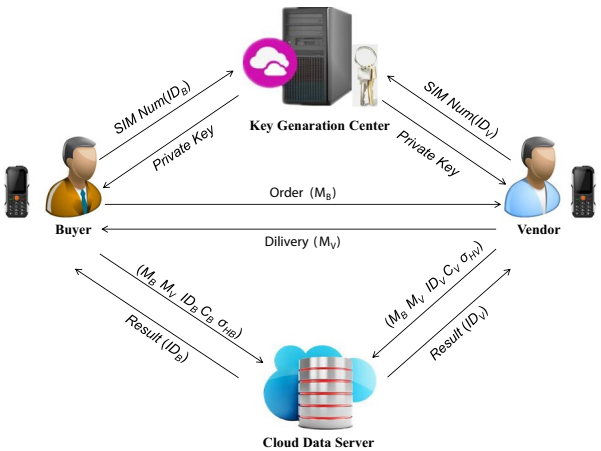

Fig. 2 System model

3.1 Our construction

The construction of IBPCE scheme comprises the following five concrete algorithms:

– $\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, \mathsf{msk})$: Taking as input a security parameter λ, this algorithm does the following:

1. Generate the pairing parameters: two groups $\mathbb{G}$ and $\mathbb{G}_\tau$ of order p, and an admissible bilinear map e.
2. At random choose generators $g, h \in \mathbb{G}$.
3. Choose two collision-resistant hash functions: $H_1 : \{0,1\}^* \to \mathcal{Z}_p^*, H_2 : \mathbb{G}_\tau \to \mathcal{Z}_p^*$.
4. At random pick $\alpha \in \mathcal{Z}_p$ and set $k = g^\alpha$.
5. Calculate $X = e(g, h)$.
6. Calculate $Y = e(g, g)$.
7. Calculate $W = e(k, h)$.
8. Set and publish the parameter

$$\mathsf{pp} = \left(p, \mathbb{G}, \mathbb{G}_\tau, e, g, h, k, H_1, H_2, X, Y, W\right)$$

9. Keep the master key $\mathsf{msk} = \alpha$.

– $\mathsf{Extract}(\mathsf{pp}, \mathsf{msk}, \mathsf{id}) \to \mathsf{pdk}_{\mathsf{id}}$: For a given identity string $\mathsf{id} \in \{0,1\}^*$, this algorithm does:

1. At random select $r_{\mathsf{id}} \in \mathcal{Z}_p^*$, and compute $t_{\mathsf{id}} = (hg^{-r_{\mathsf{id}}})^{\frac{1}{\alpha - H_1(\mathsf{id})}}$.
2. Set the private decryption key $\mathsf{pdk}_{\mathsf{id}} = (r_{\mathsf{id}}, t_{\mathsf{id}})$.

– $\mathsf{Encrypt}(\mathsf{pp}, \mathsf{id}, M) \to \mathsf{ct}$: To encrypt a message $M \in \mathcal{M}$ under identity id, this algorithm performs as following:

1. Select random number $s \in \mathcal{Z}_p$.
2. Compute $C_1 = k^s g^{-sH_1(\mathsf{id})} = g^{s(\alpha - H_1(\mathsf{id}))}$.
3. Compute $C_2 = Y^s$.
4. Compute $C_3 = M \cdot X^{-s}$.
5. Compute $C_4 = W^{s + H_2(C_2)}$.
6. Return the ciphertext $\mathsf{ct} = (C_1, C_2, C_3, C_4)$.

– $\mathsf{Decrypt}(\mathsf{pp}, \mathsf{ct}, \mathsf{pdk}_{\mathsf{id}})$: On input the system parameter pp, a ciphertext ct and a decryption key $\mathsf{pdk}_{\mathsf{id}}$, the decryption algorithm performs the following:

1. Parse the ciphertext as $\mathsf{ct} = (C_1, C_2, C_3, C_4)$, and check whether C_1 is an element in $\mathbb{G}$ and C_2, C_3 and C_4 are elements in $\mathbb{G}_\tau$. Return $\perp$ as ill-formed if the checks fail.
2. Parse the key as $\mathsf{pdk}_{\mathsf{id}} = (r_{\mathsf{id}}, t_{\mathsf{id}})$, and check whether $r_{\mathsf{id}} \in \mathcal{Z}_p^*$ and $t_{\mathsf{id}} \in \mathbb{G}$ hold. Return $\perp$ as ill-formed if the checks fail.
3. Compute and return $M = e(t_{\mathsf{id}}, C_1) C_2^{r_{\mathsf{id}}} C_3$.

Remark 1 (**Correctness of decryption**). Assuming the ciphertext and decryption key are well-formed, then

$$\begin{aligned} & e(t_{\mathsf{id}}, C_1) C_2^{r_{\mathsf{id}}} C_3 \\ &= e((hg^{-r_{\mathsf{id}}})^{\frac{1}{\alpha - H_1(\mathsf{id})}}, g^{s(\alpha - H_1(\mathsf{id}))}) e(g,g)^{r_{\mathsf{id}} s} \cdot M e(g,h)^{-s} \\ &= M \cdot e(hg^{-r_{\mathsf{id}}}, g^s) e(g,g)^{r_{\mathsf{id}} s} e(g,h)^{-s} \\ &= M \cdot e(g,h)^s e(g,g)^{-r_{\mathsf{id}} s} e(g,g)^{r_{\mathsf{id}} s} e(g,h)^{-s} \\ &= M \end{aligned} \tag{2}$$

– $\mathsf{Check}(\mathsf{pp}, \mathsf{ct}, \mathsf{id}, M) \to 1/0$: To decide whether ct is the encryption of message M under identity id, this algorithm checks the equation

$$C_4 = e(C_1, h) \cdot W^{H_2(C_2)} \left(\frac{M}{C_3}\right)^{H_1(\mathsf{id})} ? \tag{3}$$

It returns 1 if the above equation holds and returns 0 otherwise.

Remark 2 (**Consistency of check algorithm**). Assuming the ciphertext components are well-formed for id, the consistency of the check is described as:

$$\begin{aligned} & e(C_1, h) \cdot W^{H_2(C_2)} \cdot \left(\frac{M}{C_3}\right)^{H_1(\mathsf{id})} \\ &= e(g^{s(\alpha - H_1(\mathsf{id}))}, h) e(g,h)^{\alpha H_2(C_2)} e(g,h)^{s H_1(\mathsf{id})} \\ &= e(g,h)^{s\alpha} e(g,h)^{\alpha H_2(C_2)} \\ &= e(g,h)^{\alpha(s + H_2(C_2))} \\ &= e(g^\alpha, h)^{s + H_2(C_2)} \\ &= C_4 \end{aligned} \tag{4}$$

3.2 Security

To demonstrate that the security of our proposed scheme is statistically unlinkable under the decisional q-augmented bilinear Diffie-Hellman exponent (q-ABDHE) assumption, we use similar technique outlined in (Gentry 2006; Han et al. 2016).

Theorem Our proposed IBPCE scheme is (t, q, ϵ)-secure, assuming that the (t', q', ϵ')-decisional q-ABDHE assumption holds in bilinear groups, and H_1 and H_2 are (t_1, ϵ_1) and (t_2, ϵ_2) collision-resistant hash functions, respectively, where

$$\begin{cases} \epsilon' = (1-\epsilon_1)(\epsilon - \frac{1}{q}) \\ t' = t + t_1 + t_2 + o(q^2 t_e) \\ q' = q+1 \end{cases} \tag{5}$$

Proof Let $\mathcal{A} = (A_1, \mathcal{A}_2)$ be an adversary that can (t, q, ϵ)-break the security of the proposed scheme. We will construct an algorithm $\mathcal{B}$ that can use $\mathcal{A}$ to solve the decisional $(q+1)$ -ABDHE problem. The challenger $\mathcal{C}$ flips an unbiased coin from $\{0,1\}$, and obtains a bit $b \in \{0,1\}$. Then, $\mathcal{C}$ sends $(g', g'_{q+2}, g_1, g_2, \ldots, g_q, Z)$ to $\mathcal{B}$, where $Z = e(g_{q+1}, g')$ when $b = 0$; otherwise, $Z = R \in \mathbb{G}_\tau$. Note that we set $g_i = g^{\alpha^i}$ in $(q+1)$-ABDHE instance. $\mathcal{B}$ will output his guess b' on b and proceeds as follows. □

Setup: $\mathcal{B}$ selects a random polynomial $f(x) \in \mathcal{Z}_p[x]$ with $f(x) = f_0 + f_1 x + \cdots + f_q x^q$ of degree q, and sets $h = g^{f(\alpha)}$, computing h from $(g, g_1, \ldots g_q)$. It sends the public parameter $\mathsf{pp} = (g, h, k, X = e(g,h), Y = e(g,g), W = e(h,k))$ to $\mathcal{A}$ where $k = g^\alpha$.

Phase 1: $\mathcal{A}$ can adaptively query the key generation oracle. $\mathcal{B}$ responds to the query on an identity $\mathsf{id} \in \{0,1\}^*$ as follows. If $H_1(\mathsf{id}) = \alpha$, $\mathcal{B}$ uses $\mathcal{A}$ to solve the decisional q-ABDHE problem immediately. Otherwise, let $F_{\mathsf{id}}(x)$ stands for $(q-1)$ -degree polynomial $\frac{f(x)-f(H_1(\mathsf{id}))}{x-H_1(\mathsf{id})}$. Obviously, $\mathcal{B}$ sets a valid secret key $(r_{\mathsf{id}}, t_{\mathsf{id}})$ for identity id since

$$\begin{cases} r_{\mathsf{id}} = f(H_1(\mathsf{id})) \\ t_{\mathsf{id}} = (hg^{-r_{\mathsf{id}}})^{\frac{1}{\alpha - H_1(\mathsf{id})}} = g^{\frac{f(\alpha)-f(H_1(\mathsf{id}))}{\alpha - H_1(\mathsf{id})}} = g^{F_{\mathsf{id}}(\alpha)} \end{cases} \tag{6}$$

$\mathcal{B}$ responds the key extraction query with the simulated secret key $\mathsf{pdk}_{\mathsf{id}} = (r_{\mathsf{id}}, t_{\mathsf{id}})$.

Challenge: The adversary $\mathcal{A}$ submits an challenged identity id' and messages (M_0, M_1) with the same length. Also, if $H_1(\mathsf{id}') = \alpha$, $\mathcal{B}$ also uses it to solve the decisional q-ABDHE problem immediately. Furthermore, if there exists an id which is selected by $\mathcal{A}$ to query secret key with $H_1(\mathsf{id}) = H_1(\mathsf{id}') \neq \alpha$, challenger $\mathcal{C}$ aborts. Otherwise, $\mathcal{B}$ flips an unbiased coin to obtain a bit $\beta \in \{0,1\}$. It computes a private decryption key $\mathsf{pdk}_{\mathsf{id}'} = (r_{\mathsf{id}'}, t_{\mathsf{id}'})$ for id' as in Phase 1.

We define

$$f'(x) = x^{q+2} \tag{7}$$

$$\begin{aligned} F'_{\mathsf{id}'}(x) &= \frac{f'(x) - f'(H_1(\mathsf{id}'))}{x - H_1(\mathsf{id}')} \\ &= F'_0 + F'_1 x + \cdots + F'_{q+1} x^{q+1} \end{aligned} \tag{8}$$

Note that $F'_{\mathsf{id}'}(x)$ is a polynomial of degree $(q+1)$. It computes

$$\begin{aligned} C_1 &= g'^{f(\alpha) - f(H_1(\mathsf{id}'))} \\ C_2 &= Z^{F'_{q+1}} \cdot e(g', \prod_{i=0}^{q} g^{\alpha^i F'_i}) \\ C_3 &= \frac{M_\beta}{e(C_1, t_{\mathsf{id}'}) \cdot (C_2)^{r_{\mathsf{id}'}}} \\ C_4 &= Z^{f_q F'(\alpha)} \cdot \prod_{i=1}^{q} e(g', g_i)^{f_{i-1} F'(\alpha)} \end{aligned} \tag{9}$$

where F'_i is the coefficient x^j of in $F'_{\mathsf{id}'}$.

It is easily to see that the above ciphertext $\mathsf{ct} = (C_1, C_2, C_3, C_4)$ is a valid challenge ciphertext for message M_β.

Let $s = (\log_g g') F'_{\mathsf{id}'}(\alpha)$. That is, $g' = g^{\frac{s}{F_{\mathsf{id}'}(\alpha)}}$. If $Z = e(g', g_{q+1}) = e(g', g^{\alpha^{q+1}})$, we have

$$\begin{aligned} C_1 &= g'^{f(\alpha) - f(H_1(\mathsf{id}'))} \\ &= g^{\frac{s(f'(\alpha) - f'(H_1(\mathsf{id}')))}{F'_{\mathsf{id}'}(\alpha)}} \\ &= g^{s(\alpha - H_1(\mathsf{id}'))} \\ &= (g^\alpha g^{-H_1(\mathsf{id}')})^s \\ &= (kg^{-H_1(\mathsf{id}')})^s \end{aligned}$$

$$\begin{aligned} C_2 &= Z^{F'_{q+1}} \cdot e(g', \prod_{i=0}^{q} g^{\alpha^i F'_i}) \\ &= e(g', g)^{F'_{q+1} \alpha^{q+1}} e(g', \prod_{i=0}^{q} g^{F'_i \alpha^i}) \\ &= e(g,g)^{\frac{sF'(\alpha)}{F'(\alpha)}} = e(g,g)^s \end{aligned}$$

$$\begin{aligned} C_3 &= \frac{M_\beta}{e(C_1, t_{\mathsf{id}'}) \cdot (C_2)^{r_{\mathsf{id}'}}} \\ &= \frac{M_\beta}{e(g,g)^{sf(\alpha) - sf(H_1(\mathsf{id}'))} e(g,g)^{sf(H_1(\mathsf{id}'))}} \\ &= M_\beta \cdot e(g, g^{f(\alpha)})^{-s} \\ &= M_\beta \cdot e(g,h)^{-s} \end{aligned}$$

$$\begin{aligned} C_4 &= Z^{f_q F'(\alpha)} \cdot \prod_{i=1}^{q} e(g', g_i)^{f_{i-1} F'(\alpha)} \\ &= \prod_{i=1}^{q+1} e(g', g)^{f_{i-1} \alpha^i F'(\alpha)} \\ &= e(k,h)^s \end{aligned}$$

Obviously, the challenge ciphertext is well-formed.

Phase 2: The adversary $\mathcal{A}_2$ makes key generation queries with the only restriction that $\mathcal{A}_2$ cannot query key generation oracle with the challenge identity id' and $\mathcal{B}$ responds the query as in Phase 1.

Guess: The adversary $\mathcal{A}$ outputs his guess β' on β. If $\beta' = \beta$, $\mathcal{B}$ outputs $b' = b = 0$ which indicates that $Z = e(g_{q+1}, g')$ in q-ABDHE instance. Otherwise, it outputs $b' = b = 1$ which indicates Z is a random element in $\mathbb{G}_\tau$.

Probability Analysis: We now give the advantage with which $\mathcal{B}$ can solve the decisional $(q+1)$-ABDHE assumption. From the simulation and response in the above reduction, we require that $\mathcal{C}$ cannot abort.

- If id' is appeared in key generation query of phase 1 with $H_1(\mathsf{id}') = H_1(\mathsf{id}) \neq \alpha$, $\mathcal{C}$ aborts. Let $\Pr[\neg abort]$ be the probability with which the challenger $\mathcal{C}$ does not abort the game. By the security and collision-resistance of hash function H_1,

$$p_0 = \Pr[\neg abort] = 1 - \epsilon_1 \tag{10}$$

- If $\beta' = \beta$ in guess phase, $\mathcal{B}$ can solve the decisional $(q+1)$-ABDHE problem and outputs 1 to indicate $b' = b = 0$. In this case, $\mathcal{A}_2$ can guess correctly with probability

$$p_1 = |\Pr[\beta' = \beta] | b' = b = 0| \geq \epsilon \tag{11}$$

- If $\beta' \neq \beta$, the simulator $\mathcal{B}$ cannot solve the decisional $(q+1)$-ABDHE problem. Since Z is uniformly random, the components C_1, C_2 and C_4 are uniformly random and independent elements in $\mathbb{G} \times \mathbb{G}_\tau^2$. In this case, $C_4 \neq e(C_1, h) W^{H_2(C_2)} (M_\beta / C_3)^{H_1 \mathsf{id}'}$ holds with the probability $1 - 1/q$. When the above inequality holds, then

$$\begin{aligned} & e(C_1, t_{\mathsf{id}'}) C_2^{r_{\mathsf{id}'}} \\ &= e(C_1, (h g^{-r_{id'}})^{\frac{1}{\alpha - H_1(\mathsf{id}')}}) \cdot C_2^{r_{\mathsf{id}'}} \\ &= e(C_1, h)^{\frac{1}{\alpha - H_1(\mathsf{id}')}} (C_2 / e(C_1, g)^{\frac{1}{\alpha - H_1(\mathsf{id}')}})^{r_{\mathsf{id}'}} \end{aligned} \tag{12}$$

As $r_{\mathsf{id}'}$ is randomly selected, C_3 is also uniformly random. Namely, the ciphertext $\mathsf{ct} = (C_1, C_2, C_3, C_4)$ can reveal no information regarding the bit β. Thus, the adversary $\mathcal{A}_2$ can guess $\beta' \neq \beta$ with probability

$$p_2 = \left| \Pr[\beta' \neq \beta | \ b' = b = 1] \right| \leq \frac{1}{q} \tag{13}$$

Thus, $\mathcal{B}$ can solve the decisional $(q+1)$-ABDHE problem with probability

$$\epsilon' = \Pr[\neg abort] \cdot |p_2 - p_1| \geq (1 - \epsilon_1)(\epsilon - \frac{1}{q}) \tag{14}$$

3.3 Time complexity

Let H_1 and H_2 are and collision-resistant hash functions, respectively. In order to response to adversary $\mathcal{A}$'s key generation query on identity id, $\mathcal{B}$'s overhead is dominated by computing $t_{\mathsf{id}} = g^{F_{\mathsf{id}}(\alpha)}$ in the phase 1. And each such computation requires $o(q)$ exponentiations. When $\mathcal{A}$ makes at most $(q-1)$ queries, the time complexity is

$$t' = t + t_1 + t_2 + o(q^2 t_e) \tag{15}$$

where t_e denotes the computation cost of an exponentiation operation.

This concludes the proof of Theorem 1 and it demonstrates that an algorithm is able to solve the decisional $(q+1)$-ABDHE problem with probability at least ϵ' and in time at most t' if an adversary can break our scheme, which is contradicted against the decisional $(q+1)$-ABDHE assumption. Thus, our proposed IBPCE scheme is secure.

3.4 Performance analysis

As shown in Table 1, the second, third and fourth rows represent the computation comparison of encryption, decryption and check algorithm, respectively. The fifth row denotes sizes of ciphertext. The following two rows indicate whether

Table 1 Performance analysis Calc Cost: calculation cost, Enc: encryption algorithm, Dec: decryption algorithm, Check: check algorithm T_{exp}: an exponentiation operation, T_{pm}: an point multiplication operation, T_{add}: an addition operation, T_h: hash function operation, T_{bp}: a bilinear pair-ing operation, $|\mathbb{G}|$: size of an element in $\mathbb{G}$, $|\mathcal{Z}_p|$: size of an element in $\mathcal{Z}_p$ (i.e., $\log p$), $|H|$: size of hash output, decisional q-ABDHE: decisional q-augmented bilinear Diffie-Hellman exponent assumption

	ACME (Han et al. 2016)	Ours
Calc cost of encryption	$6T_{exp} + 3T_{pm} + 2T_h$	$5T_{exp} + 3T_{pm} + 2T_h + T_{add}$
Calc cost of decryption	$2T_{pm} + T_{bp} + T_{exp}$	$2T_{pm} + T_{bp} + T_{exp}$
Calc cost of check	$3T_{pm} + 2T_{exp} + 2T_h + 2T_{bp}$	$3T_{pm} + 2T_{exp} + 2T_h + T_{bp}$
Size of ciphertext	$3\|\mathbb{G}_\tau\| + \|\mathbb{G}\| + \|H\|$	$3\|\mathbb{G}_\tau\| + \|\mathbb{G}\|$
Size of Key	$\|\mathbb{G}\| + \|\mathcal{Z}_p\|$	$\|\mathbb{G}\| + \|\mathcal{Z}_p\|$
Plaintext checkable	Yes	Yes
Standard model	Yes	Yes
Security assumption	q-ABDHE	Decisional q-ABDHE

the schemes are plaintext checkable and proved under the standard model respectively. The last row shows the security assumptions.

In terms of computing complexity, the encryption and check phases of our scheme are decreased in comparison with Han et al.'s IBPCE scheme (Han et al. 2016), respectively. However, the decryption phases of our scheme is same with that in (Han et al. 2016). And in terms of storage, the size of ciphertext in our IBPCE scheme is shorter than that of (Han et al. 2016). Additionally, both schemes provide plaintext check, and both of them are proven secure based on the decisional q-ABDHE assumption in the standard model.

4 Accountable mobile E-commerce

To guarantee the security of mobile e-commerce, in this section, we exploit the proposed IBPCE scheme and an efficient IBS scheme (Ma et al. 2015) incorporated into the mobile e-commerce scenario which generates an accountable mobile e-commerce scheme. We first introduce the interaction between mobile client and cloud server. Then, we present our proposed accountable mobile e-commerce scheme. Figure 3 demonstrates the process of our proposed accountable mobile e-commerce scheme.

After a user finishing his registration and login, he can gain access to the system and choose services/goods according to personal needs. These services or goods on the web page are presented in a dynamic form, and the user selects the transaction on demand. At this point, the system requires users to fill in some necessary information for recording the transaction process, and sends these encrypted information to the server and generate sessions. Certainly, the above transaction requests, encrypted information and the response data will be packaged into transaction data returned to user for viewing.

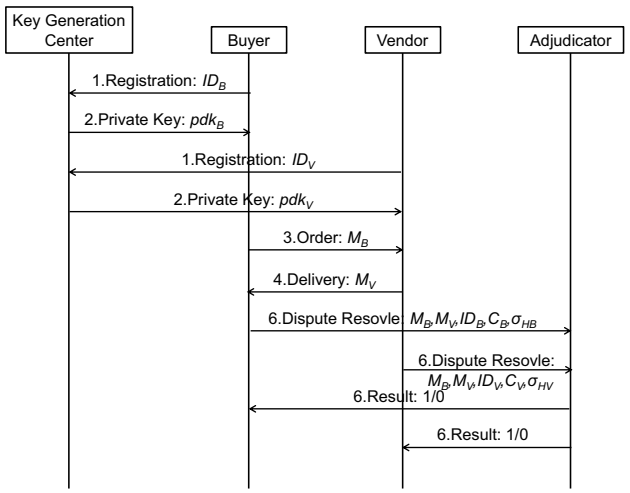

Fig. 3 Protocol of accountable mobile e-commerce

Before returning the data, the server will judge information that the user has filled out and the service selected by user, dynamically generate the specific transaction flow for user and guide to complete transaction.

– Setup (1^λ):

1. Taking as input a system security parameter, generate bilinear description $(e, p, \mathbb{G}, \mathbb{G}_\tau) \leftarrow \mathcal{G}(1^\lambda)$.
2. At random pick two generators $g, h \in \mathbb{G}$, and three collision-resistant hash functions $H_1 : \{0,1\}^* \rightarrow \mathcal{Z}_p$, $H_2 : \mathbb{G}_\tau \rightarrow \mathcal{Z}_p^*$, and $H_3 : \{0,1\}^* \rightarrow \mathcal{M}$ where $\mathcal{M}$ denotes the message space.
3. Select $\alpha \in \mathcal{Z}_p$ and set $k = g^\alpha$.
4. Run the algorithm IBS.Setup to create (IBS.pp, IBS.msk).
5. Set and keep the master private key (α, IBS.msk).
6. Publish the parameter

$$\mathsf{pp} = \Big(\mathsf{IBS.pp}, (e, p, \mathbb{G}, \mathbb{G}_\tau), g, h, k, X = e(g,h), Y = e(g,g), W = e(k,h)\Big)$$

– User Register $(\mathsf{pp}, \mathsf{id}_U) \rightarrow \mathsf{pdk}_U$:

1. Submit user's mobile phone number or email address $\mathsf{id}_U \in \{0,1\}^*$.
2. Select a randomness $r_U \in \mathcal{Z}_p$, and then compute $t_U = (hg^{-r_U})^{1/(\alpha - H_1(\mathsf{id}_U))}$.
3. Run the algorithm IBS.Extract to obtain the key sk_U.
4. Generate and output the user's decryption key $\mathsf{pdk}_U = (r_U, t_U, \mathsf{sk}_U)$.

- Order $(\mathsf{pp}, \mathsf{id}_V, M_B)$: To order a service or personal belongings from vendor's description $M_B \in \mathcal{M}$, the order algorithm does as follows:

1. At random select $s_B \in \mathcal{Z}_p$, and compute $C_{B_1} = (kg^{-H_1(N_V)})$, $C_{B_2} = Y^{s_B}$, $C_{B_3} = M_B \cdot X^{-s_B}$, $C_4 = W^{s_B + H_2(C_{B_2})}$.
2. Set the ciphertext as $\mathsf{ct}_B = (C_{B_1}, C_{B_2}, C_{B_3}, C_{B_4})$.
3. Compute $HB_1 = H_3(\mathsf{ct}_B)$.
4. Run the signing algorithm IBS.Sign(IBS.pp, HB_1, sk_B) to obtain the signature σ_{HB_1}.
5. Send $(\mathsf{ct}_B, \sigma_{HB_1})$ to the vendor.

– Delivery: To send service or personal belongings where the buyer ordered, the delivery protocol proceeds as follows:

1. Compute $HV_1 = H_3(\mathsf{ct}_B)$,
2. Run the IBS verifying algorithm to check

   $\mathsf{IBS.Verify}(\mathsf{IBS}.pp, HV_1, \mathsf{id}_B, \sigma_{HB_1}) = 1?$

   If check fail, return $\perp$ and the protocol fail.
3. Calculate $M_B = e(t_V, C_{B_1}) \cdot C_{B_2}^{r_V} \cdot C_{B_3}$.
4. Pick $s_V \in \mathcal{Z}_p$ randomly, and calculate $C_{V_1} = (kg^{-H_1(N_B)})^{s_V}$, $C_{V_2} = Y^{s_V}$, $C_{V_3} = M_V \cdot X^{-s_V}$, $C_{V_4} = W^{s_V + H_2(C_{V_2})}$, where $M_V \in \mathbb{G}_\tau$ is the buyer required.
5. Set the ciphertext $\mathsf{ct}_V = (C_{V_1}, C_{V_2}, C_{V_3}, C_{V_4})$.
6. Calculate $HV_2 = H_3(\mathsf{ct}_V)$.
7. Run the algorithm $\mathsf{IBS.Sign}(\mathsf{IBS.pp}, HV_2, \mathsf{sk}_V)$ to obtain the signature σ_{HV_2}.
8. Finally, send $(\mathsf{ct}_V, \sigma_{HV_2})$ to the buyer.

– Retrieve $(\mathsf{pp}, \mathsf{ct}_V, \mathsf{pdk}_B) \rightarrow M_V$: To retrieve order confirmation, the retrieve algorithm does as follows:

1. Calculate $HB_2 = H_3(\mathsf{ct}_V)$.
2. Run the verifying algorithm to check

   $\mathsf{IBS.Verify}(\mathsf{IBS.pp}, \mathsf{id}_V, HB_2, \sigma_{HV_2}) = 1?$

   If fail, return $\perp$ and stop the protocol.
3. Return $M_V = e(t_B, C_{V_1}) \cdot C_{V_2}^{r_B} \cdot C_{V_3}$.

– Payment: After confirming the received personal belongings or services, the system transfers the buyer's payments from a third-party payment platform to the vendor, and finishes the transaction.
– Dispute Settlement $(\mathsf{pp}, \mathsf{ct}, \mathsf{id}_U, M)$: To deal with the possible dispute, the adjudicator does as follows:

1. Require the buyer to send $(M_B, M_V, \mathsf{id}_B, \mathsf{ct}_B, \sigma_{HB})$ and the vendor to send $(M_B, M_V, \mathsf{id}_V, \mathsf{ct}_V, \sigma_{HV})$ the adjudicator, respectively.
2. Parse $\mathsf{ct}_B = (C_{B_1}, C_{B_2}, C_{B_3}, c_{B_4}) \in \mathbb{G} \times \mathbb{G}_\tau^3$, and $\mathsf{ct}_V = (C_{V_1}, C_{V_2}, C_{V_3}, c_{V_4}) \in \mathbb{G} \times \mathbb{G}_\tau^3$.
3. Calculate $HB = H_3(\mathsf{ct}_B)$ and $HV = H_3(\mathsf{ct}_V)$.
4. Check the following equations:

$$\mathsf{IBS.Verify}(\mathsf{pp}, \mathsf{id}_B, HB, \sigma_{HB}) = 1 \tag{16}$$

$$C_{B_4} = e(C_{B_1}, h) \cdot W^{H_2(C_{B_2})}(M_B / C_{B_3})^{H_1(\mathsf{id}_V)} \tag{17}$$

$$\mathsf{IBS.Verify}(\mathsf{pp}, \mathsf{id}_V, HV, \sigma_{HV}) = 1 \tag{18}$$

$$C_{V_4} = e(C_{V_1}, h) \cdot W^{H_2(C_{V_2})}(M_V / C_{V_3})^{H_1(\mathsf{id}_B)} \tag{19}$$

5. If both eqs. (16) and (17) hold, the buyer is honest. Otherwise it is dishonest. If both eqs. (18) and (19) hold, the vendor is honest. Otherwise it is dishonest.

5 Performance evaluation

In this section, we evaluate the performance of the proposed accountable mobile e-commerce and the Han et al.'s AMEC scheme (Han et al. 2016), in terms of the computation and communication complexity. It is mentioned that Han et al.'s AMEC scheme is derived from their proposed IBPCE scheme and Patson et al.'s IBS scheme (Paterson and Schuldt 2006). We not only propose our IBPCE scheme in section 3.1 and make a comparison in section 3.3, but also use an IBS scheme which is proved to be more efficient than Patson et al.'s. Therefore, we are not going to repeat that comparison between the two IBS schemes. We compare the other part of AMEC scheme which is derived from our proposed IBPCE scheme.

5.1 Computation cost and experiments

The comparison of computing costs is presented in Table 2, which includes different phases, such as order, delivery, retrieve and dispute etc.

The running time is described in Table 3. To obtain the execution time of the basic operations in the two schemes, we conduct the experiment with MIRACL libraries (2017) running on a 2.30 GHz-processor and 1 GB-memory

Table 2 Computation complexity

Protocols	ACME (Han et al. 2016)	Ours
Order	$6Texp + 3T_{pm} + 2T_h$	$5Texp + 3T_{pm} + 2T_h + T_{add}$
Delivery	$7Texp + 5T_{pm} + 2T_h + T_{bp}$	$6Texp + 5T_{pm} + 2T_h + T_{bp} + T_{add}$
Retrieve	$Texp + 2T_{pm} + T_{bp}$	$Texp + 2T_{pm} + T_{bp}$
Dispute Settlement	$4Texp + 6T_{pm} + 4T_h + 4T_{bp}$	$4Texp + 6T_{pm} + 4T_h + 2T_{bp}$

Table 3 Running time of different operations

Operation	Denotation	Time (ms)
T_{exp}	Exponentiation operation	0.331
T_{pm}	Point multiplication	1.97
T_h	Hash function	0.011
T_{add}	Addition operation	0.012
T_{bp}	Bilinear map	5.275

computing machine. The experimental results listed in Table 3.

We provide the comparison of computation costs in Figure 4 based on the above execution time by graph so as to reflect the difference intuitively.

From the results in Fig. 4, it is obviously to show that the computation costs in Order, Delivery and dispute settlement phases of our scheme decrease by 4.03%, 1.46% and 30.80% as compared to that of AMEC scheme (Han et al. 2016), respectively. Even though the computation cost in the Cost and Delivery phase of our scheme is a little bit lower than that in (Han et al. 2016), these two parts would not be used by cloud server in the processing of identifying users who is dishonest. Therefore, our scheme achieves a better computation efficiency compared to that of AMEC scheme.

5.2 Communication cost

To achieve the similar security level of 1024-bit RSA (or AES-80), it should satisfy $l \times \omega \geq 1024$ where l is the group size of elliptic curve and ω is embedding degree. When evaluating communication performance of our scheme, we select Type-A curve with $l = 512$-bit, and a 160-bit length prime order p. In this way, the elements in $\mathbb{G}$ and $\mathbb{G}_\tau$ are 64 bytes (512-bit) and 128 bytes (1024-bit), respectively. Besides, we choose SHA-1 as the collision-resistant hash function. The comparison of communication complexity is presented in Figure 4, and the communication costs in Figure 5.

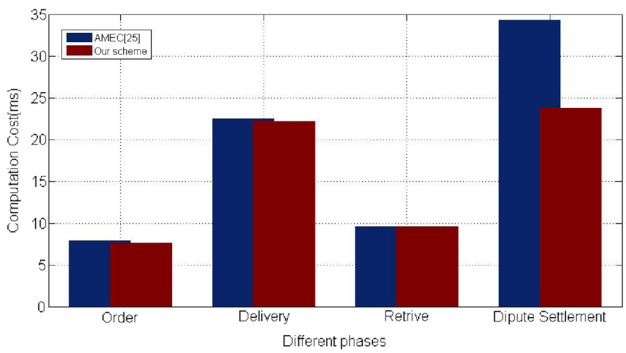

Fig. 4 Computation comparison in different phases

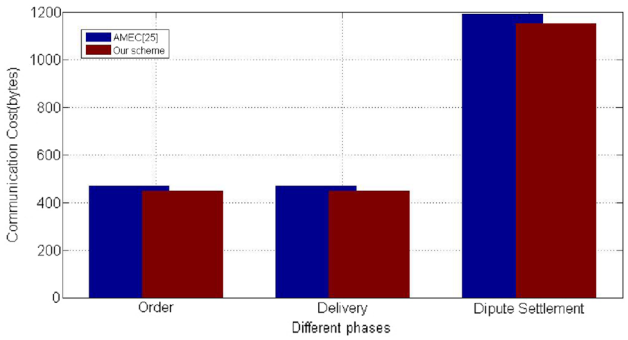

Fig. 5 Communication cost

From the results in figures 4 and 5, it is easily to indicate that communication costs of our scheme are a little bit lower than AMEC scheme in generally. Our scheme can provide the security of the user's private information and resolve possible disputes, and since the combined scheme has been proved more efficient than Paterson et al.'s (Paterson and Schuldt 2006) used in scheme (Han et al. 2016), the efficiency of our scheme has a greater improvement advantage compared with previous schemes.

6 Conclusion

We presented a mobile e-commerce transaction based on cloud computing for intelligent information services and we also proposed an accountable mobile e-commerce scheme to take the transaction in this open and distributed intelligent systems. We gave the concrete construction of the scheme and analyzed the security. Compared with related scheme, our scheme is more practical and efficient.

Acknowledgements This work is supported by the National Natural Science Foundation of China under grants 61672010, 61370224 and 61702168, and the Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes of Guangzhou University.

References

Biswas D, Vidyasankar K (2014) Privacy preserving and transactional advertising for mobile services. Computing 96(7):613–630

Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing. In: Advances in Cryptology-CRYPTO 2001, Springer, pp 213–229

Brown A, Mortier R, Rodden T (2012) Multinet: usable and secure wifi device association. ACM SIGCOMM Comput Commun Rev 42(4):275–276

Buyya R, Yeo CS, Venugopal S (2008) Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In: High Performance Computing and

Communications, 2008. HPCC'08. 10th IEEE International Conference on, IEEE, pp 5–13
Canard S, Fuchsbauer G, Gouget A, Laguillaumie F (2012) Plaintext-checkable encryption. Topics in Cryptology-CT-RSA 2012:332–348
Duarte M, Sabharwal A, Aggarwal V, Jana R, Ramakrishnan K, Rice CW, Shankaranarayanan N (2012) Design and characterization of a full-duplex multiantenna system for wifi networks. IEEE Trans Vehicular Technol 63(3):1160–1177
Fu Z, Wu X, Guan C, Sun X, Ren K (2016) Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur 11(12):2706–2716
Gentry C (2006) Practical identity-based encryption without random oracles. Eurocrypt, Springer 4004:445–464
Ghosh AK, Swaminatha TM (2001) Software security and privacy risks in mobile e-commerce. Commun ACM 44(2):51–57
Han CK, Choi HK (2013) Security analysis of handover key management in 4g lte/sae networks. IEEE Trans Mobile Comput 13(2):457–468
Han J, Yang Y, Huang X, Yuen TH, Li J, Cao J (2016) Accountable mobile e-commerce scheme via identity-based plaintext-checkable encryption. Inf Sci 345:143–155
Hwang RH, Huang CF, Lin CH, Chung CY (2015) Context-aware multimedia broadcast and multicast service area planning in 4g networks. Comput Commun 64:33–43
Jo HJ, Paik JH, Lee DH (2014) Efficient privacy-preserving authentication in wireless mobile networks. IEEE Trans Mobile Comput 13(7):1469–1481
Kim Y, Shin H, Chon Y, Cha H (2015) Crowdsensing-based wi-fi radio map management using a lightweight site survey. Comput Commun 60:86–96
Kolodziej J, Xhafa F (2011) Supporting situated computing with intelligent multi-agent systems. Int J Space-Based Situated Comput 1(1):30–42
Ma S (2016) Identity-based encryption with outsourced equality test in cloud computing. Inf Sci 328:389–402
Ma S, Huang Q, Zhang M, Yang B (2015) Efficient public key encryption with equality test supporting flexible authorization. IEEE Trans Inf Forensics Secur 10(3):458–470
Miracl L (2017) Miracl cryptographic library: multiprecision integer and rational arithmetic c/c++ library. https://www.miracl.com/
Park JH, Lee DH (2016) An efficient ibe scheme with tight security reduction in the random oracle model. Des, Codes Cryptogr 79(1):63–85
Paterson KG, Schuldt JC (2006) Efficient identity-based signatures secure in the standard model. In: Australasian Conference on Information Security and Privacy, Springer, pp 207–222
Seo JH, Emura K (2014) Revocable hierarchical identity-based encryption. Theor Comput Sci 542:44–62
Shamir A et al (1984) Identity-based cryptosystems and signature schemes. Crypto, Springer 84:47–53
Shen J, Chang S, Shen J, Liu Q, Sun X (2016) A lightweight multilayer authentication protocol for wireless body area networks. Future Generation Comput Syst 78:956–963
Shen J, Shen J, Chen X, Huang X, Susilo W (2017) An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Transactions on Information Forensics and Security
Tang C, Wu DO (2008) Mobile privacy in wireless networks-revisited. IEEE Trans Wireless Commun 7(3):1035–1042
Torres-Sospedra J, Montoliu R, Trilles S, scar Belmonte, Huerta J, (2015) Comprehensive analysis of distance and similarity measures for wi-fi fingerprinting indoor positioning systems. Expert Systems with Applications 42(23):9263–9278
Varshney U, Jain R (2001) Issues in emerging 4g wireless networks. Computer 34(6):94–96
Wang S (2007) Practical identity-based encryption (ibe) in multiple pkg environments and its applications. arXiv preprint cs/0703106
Waters B (2005) Efficient identity-based encryption without random oracles. Eurocrypt, Springer 3494:114–127
Xia Z, Wang X, Sun X, Wang Q (2015) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel and Distributed Syst 27(2):340–352
Yang B, Liu H (2010) Cloud computing is a driving force for mobile internet development. Telicom Eng Technics Stand 23(12):24–27
Yang J, Zheng Y (2012) Reconstruction of traditional e-commerce system based on workflow technology. In: Computer Science and Network Technology (ICCSNT), 2011 International Conference on, IEEE, vol 3, pp 1927–1931
Ye S, Xiao L (2013) Designation and realization of mobile commerce interaction model under cloud computing platform. Comput Sci 40(6A):247–250
Zhang M, Mu Y (2016) Token-leakage tolerant and vector obfuscated ipe and application in privacy- preserving two-party point/polynomial evaluations. Comput J 59(4):493–507
Zhu S, Yang X (2015) Protecting data in cloud environment with attribute-based encryption. Int J Grid Utility Comput 6(2):91–97