Soft Computing
https://doi.org/10.1007/s00500-018-3159-0

METHODOLOGIES AND APPLICATION

Identity-based undetachable digital signature for mobile agents in electronic commerce

Yang Shi[1] · Jingxuan Han[1] · Jiangfeng Li[1] · Guoyue Xiong[1] · Qinpei Zhao[1]

Abstract

To enable mobile agents signing securely on potentially malicious hosts in electronic commerce and other applications, we proposed the definition and security notion of identity-based undetachable digital signature schemes. More importantly, we proposed a concrete identity-based undetachable digital signature scheme with provable security. In the scheme, mobile agents need not carry the private key when they generate digital signatures on behalf of the original signer, so the private key will not be compromised. The encrypted function is combined with the original signer's requirement, so misuse of the signing algorithm can be prevented. Moreover, because the scheme is identity-based, verification of the signatures generated by mobile agents does not require either verification of the entire certificate path or communication with the certification authority. Therefore, compared with existing undetachable signature schemes, the cost of verification is reduced and even the dependence on a stable network connection is weakened.

Keywords Mobile agents · Identity-based · Undetachable digital signatures · Electronic commerce

1 Introduction

With the development in technologies of distributed computing, mobile agent technologies and systems have attracted great interest. Commonly, a mobile agent system comprises platforms and mobile agents. Agents are a type of computer software acting autonomously on behalf of an organization or a person (Object Management Group 1997). Meanwhile, platforms are agent systems that can generate, execute, transfer, and terminate agents. Like an agent, an agent system is associated with an authority identifying the organization or person for which the agent system acts. Moreover, agent systems operate on computers connected by networks and can exchange information with each other via a communication infrastructure. While static agents may reside on hosting platform or an immobile system, mobile agents can transport themselves easily from one platform in a network to another. They can also automatically suspend execution on one platform and migrate to another to restart their computations. The capability of them to travel enables a mobile agent to migrate to a destination agent system that contains an entity in which the agent wishes to interact. Furthermore, the mobile agent may utilize the destination agent platform's services.

The advent of electronic business practices has significantly increased the demand for flexibility in distributed computing environments and interoperability to enable real-time exchange of data across enterprise borders, across applications, and across IT platforms. Compared with traditional computing models (e.g., client/server), mobile agent technology has several significant advantages in electronic commerce applications (Busch et al. 1998; Singh and Dave 2013). First, autonomous mobile agents strive to achieve a given goal without continuous supervision by the owner of the agent. Second, when a host is shut down, all mobile agents running on that machine are warned and given time to dispatch; they then continue their operation on another host in the network. Third, users may dispatch agents to a target host via a temporary network connection. After the agent is dispatched, the temporary network connection can be brought down until a later time.

In electronic commerce, an intelligent mobile agent that roams the Internet to purchase services or goods on behalf of its owner usually has many advantages. It can specifically allow businesses to respond rapidly to market opportunities

Communicated by V. Loia.

✉ Qinpei Zhao
qinpeizhao@tongji.edu.cn

[1] Tongji University, Shanghai 201804, People's Republic of China

Published online: 23 March 2018

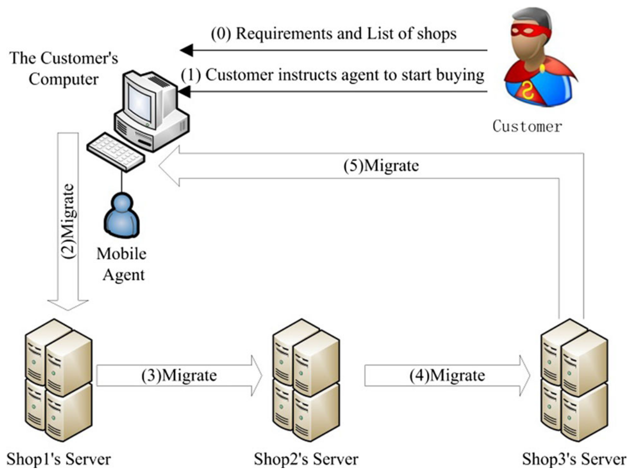


Fig. 1 Intelligent trade agent roaming a network

and give the competitive edge that is required in business world of today to them. Figure 1 illustrates an intelligent trade agent that roams the Internet buying services or goods from the hosts of three shops in the network.

Furthermore, a number of mobile agent-based technologies are developed and put into practice. In Chung et al. (2011), an agent-based English auction protocol was introduced for mobile commerce that allows the bidders to take part into the online auctions by using mobile agents. A silicon intellectual property service and trading platform was proposed in Trappey et al. (2006). A hybrid multi-agent negotiation protocol was provided by Wang et al. supporting agent mobility in virtual enterprises (2014), and an autonomous trading system was proposed by Du et al. in electronic marketplace (2005). An architecture that was based on mobile agents allowing the users to do business anywhere and anytime via their mobile devices was introduced in Aloui et al. (2012). An extended contract-net-like multilateral protocol (ECNPro) for multilateral contract negotiations in supply chain management was presented in Wong and Fang (2010).

These applications cannot be securely implemented without appropriate technologies to guarantee that sensitive business data are appropriately protected and business partners can work together with integrity and confidence. Mobile agents are easily exposed to serious security threats. One glaring threat is that malicious hosts might endanger passing agents, because such agents operate in a white-box attack context (WBAC) on these hosts (Shi et al. 2011). As security threats from malicious hosts have become a bottleneck in the application of mobile agent systems, there is an urgent calling for practical and efficient security countermeasures that can achieve both mobility and security in studies of mobile agent. This paper proposes an identity-based undetachable digital signature scheme as a useful security countermeasure.

The remainder of this paper is organized as follows. The next section presents a brief introduction to the threats against the security of mobile agents. The section also provides background information about WBACs. Section 3 proposes a definition of identity-based undetachable digital signature schemes and a corresponding security model. Section 4 proposes and analyzes the construction of a new identity-based undetachable digital signature scheme. Section 5 compares the scheme in this paper with other undetachable digital signature schemes. Finally, the article concludes with a discussion of the findings.

2 Backgrounds and motivations

2.1 Security threats on mobile agent systems

As we have previously discussed, mobile agent technology offers significant benefits for electronic commerce. However, it also brings an issue which is security. Specifically, threats to the security of mobile agents generally fall into four comprehensive classes (Jansen 2000): (1) agent-against-agent-platform; (2) agent-platform-against-agent; (3) agent-against-other-agents; and (4) other-entities-against-agent-system.

There are many reasons that can lead a host to attack the agents that is executing (Esparza et al. 2011). Note that "platform" and "host" is used interchangeably to refer a place where mobile agents operate. The host can try to obtain an economical benefit or a favorable execution, or it can just try to damage the reputation of another principal. The protection of mobile agents against attacks from platforms (malicious hosts) is referred to as the problem of malicious hosts. A mobile agent is in a WBAC if it is running on a malicious hosts. A WBAC is a dangerous computing environment in which applications (e.g., agents) are subject to full-privilege attacks from the execution platform. Secure computing in WBACs (e.g., in malicious hosts) is a challenge, because the adversary can (De Mulder et al. 2013): (1) trace every instruction of the executable implementation, (2) view the contents of cache and memory, (3) stop or pause execution at any point and run an online process, and (4) alter code or memory contents at will.

Thus, security issues, especially threats from malicious hosts, have become a great obstacle to the widespread deployment of applications in electronic commerce that was based on mobile agents.

2.2 Digital signature of mobile agents under white-box attack context

In traditional signature schemes, a mobile agent needs to carry the implementation of the signing algorithm with the

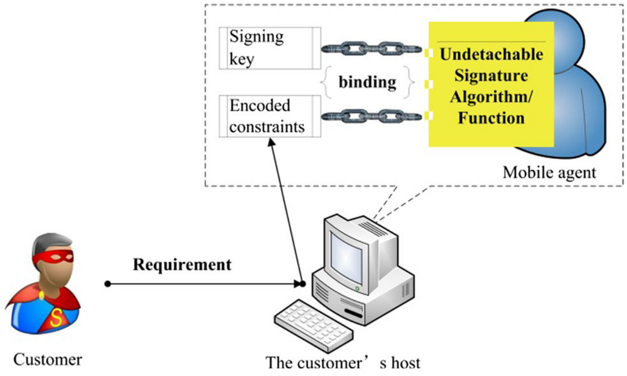


Fig. 2 The principle of undetachable digital signature

private signing key to generate digital signatures on behalf of the original user, so an adversary can misuse the signing algorithm or even extract the signing key from the agent in WBACs. This is why Sander and Tschudin presented the idea of undetachable digital signatures (1998), which allows a mobile agent to generate a digital signature effectively even inside a remote malicious host without the host being able to deduce the agent's secret (for example, the private key) or misuse the signing algorithm's implementation for arbitrary information. The mechanism is to encode constraints into the implementation of the signing algorithm avoiding the explicit use of the original signing key. A constraint is a limitation or like a restriction "a ThinkPak portable PC costs no more than 1588 Dollars." If the constraints are not satisfied, a valid signature is not generated, which prevents arbitrary messages from being signed. Their main idea is demonstrated in Fig. 2.

The general mathematical description of an undetachable signature function is as follows. First, let Sig be a function used by C (a customer) to produce the digital signature $z = Sig(m)$ for an arbitrary message m. Next, suppose the message m is the result of a function f applied to an input data x. The function f could, for example, add each document a prefix saying that the following digitally signed order form is valid only when the document satisfies the restriction (e.g., "a Note IV smart phone costing no more than 626 Dollars.") To create undetachable signatures from the customer's mobile agent, Eq. (1) is computed, and f_{Signed} and f are both sent to S (a shop), where,

$$f_{Signed} = Sig \circ f \tag{1}$$

S then evaluates Eq. (2).

$$z = f_{Signed}(m) \tag{2}$$

Everyone can verify the validity of message m by using a specialized verification algorithm, although the signature function Sig is not known by others.

Kotzanikolaou et al. (2000) presented an undetachable digital signature scheme based on the well-known RSA cryptosystem. This is the first concrete construction of an undetachable digital signature. Since (Kotzanikolaou et al. 2000) was published, a variety of undetachable signature schemes have been proposed. The latest one is a forward-secure undetachable signature scheme (Shi et al. 2015) proposed in 2015. In Sect. 5, we briefly study and compare these schemes with our scheme.

2.3 Identity-based signatures

In a traditional public key cryptosystem, the association between a user's identity and his/her public key is obtained through a digital certificate issued by a certification authority (CA). The process of certificate management requires high computational and storage efforts. To simplify this process, Shamir (1985) introduced the concept of identity-based cryptosystem. In such cryptosystems, a user's public key is derived from his/her identity and the corresponding secret key is generated by a trusted authority (TA). The advantage of identity-based cryptosystems is that they simplify the key management process which is a heavy burden in certificate-based cryptosystems. In an identity-based cryptosystem, the verifier can verify a signature of the signer just by using the signer's identity. It only requires a directory for authenticated public system parameters of the key distribution center (KDC), which is clearly less burdensome than maintaining a public key directory for all users.

However, in an identity-based cryptosystem, the leakage of a private key is a disaster to the corresponding user, because the public key is his/her identity (or derived from the identity), and the private key cannot be updated with changing the public key. Thus, the protection of private keys in an identity-based cryptosystem is more important than that in a certification-based cryptosystem.

To the best of our knowledge, all published works on undetachable digital signatures are certification-based. This means that when a verification algorithm is running, usually a network connection to the CA or KDC is needed. Motivated by the above requirements, we propose the identity-based undetachable digital signature to fix the research gap. The proposed identity-based undetachable digital signature techniques provide a countermeasure against the threats of private key leakage and signing algorithm misusing of an identity-based cryptosystem in a WBAC (e.g., on a malicious host). At the same time, the countermeasure is independent on a long-term connectivity to the CA or KDC, because it uses identity-based techniques. With an identity-based undetachable digital signature scheme, we can achieve a good balance between fault tolerance and security in the applications of mobile agents.

One of the main contributions of this paper is to introduce the definition and security notion of identity-based undetachable digital signature schemes. More importantly, we propose a concrete identity-based undetachable digital signature scheme. To verify the scheme, security proofs are also given.

3 Definition and security notions of identity-based undetachable signature

In this section, a definition of identity-based undetachable digital signature schemes is proposed. Moreover, the security notions of the schemes are given.

3.1 Definition

An identity-based undetachable signature scheme consists of seven algorithms as follows:

KGen This is the common key generation algorithm that generates the master secret key and system parameters. The input is a security parameter 1^k, where $k \in \mathbb{N}$. The algorithm outputs system parameters Ω and a master secret key s in polynomial time. The algorithm is probabilistic.

Extract The input is an identity ID and the master secrete key s; the algorithm outputs the private key sk_{ID} in polynomial time.

UndSigFunGen The undetachable signing function generation algorithm $UndSigFunGen$ is a probabilistic polynomial-time (PPT) algorithm, which takes the requirement of a customer REQ_C, the customer's identity ID_C, and the customer's public key and private key as inputs. The algorithm outputs (an implementation of) the function $f_{Signed}(\cdot)$.

IDUndSig The undetachable signing algorithm $IDUndSig$ takes a contract (or a corresponding hash value) as input. The algorithm outputs an undetachable digital signature z in polynomial time.

IDUndVrfy The undetachable signature verification algorithm $IDUndVrfy$ takes a contract and the undetachable signature z as input. The algorithm outputs either 1 (accept) or 0 (reject) in polynomial time.

IDSig The identity-based signing algorithm $IDSig$ is a PPT algorithm, which takes input a message Msg, a signer's identity ID (or the signer's public key) and the signer's private key sk_{ID}, and then outputs a signature on the message.

IDVer The identity-based verification algorithm $IDVer$ is a polynomial-time algorithm that takes as input the signer's identity ID, a message Msg, and a digital signature, and outputs either "Accept" or "Reject"—simply 1 or 0.

As illustrated in Fig. 3, an identity-based undetachable digital signature scheme typically works as follows. First, a trusted authority (TA), such as a KDC, should publish all public parameters of the cryptosystem to all participants by running $KGen(1^k)$. Then, the TA runs the algorithm $Extract(ID)$ several times and sends private keys to each participant via a correspondingly secure communication channel. When a customer wants a mobile agent to "do some shopping" on the customer's behalf, the customer runs the algorithm $UndSigFunGen$ to prepare the mobile agent before the agent starts migrating. At the same time, sensitive data such as the customer's requirement REQ_C should be signed using $IDSig$. Then, the mobile agent starts migrating to look for shops that are willing to satisfy the customer's requirement. When a mobile agent arrives on behalf of a customer, the shop's server should first verify the integrity of the data carried by the mobile agent using the identity-based verification algorithm $IDVer$. Then, if the shop's owner or an intelligent selling agent representing the owner is willing to make a deal with the customer, the owner or agent should run the algorithm $IDUndSig$ to generate a signature on the contract. Finally, anyone can check the validity of a contract using the algorithm $IDUndVrfy$.

3.2 Security notions

While an adversary tries to attack a signature scheme, the expected results are classified in three categories as follows: The first is termed total break—that is, the adversary obtains the private key of the signer. It is the most significant result. The second is called universal forgery. In this case, the adversary acquires the ability of sign any message. The third is called existential universal forgery (EUF), in which the adversary is able to provide a new message–signature pair. In some cases, EUF is not dangerous, because the output message is likely to be meaningless. Nevertheless, a signature scheme that is not existentially unforgeable cannot guarantee, by itself, the identity of the signer. For example, it cannot be used to certify ostensibly random elements, such as keys.

In addition to the result that an adversary can achieve, the adversary's capabilities are also important for measuring the security of a signature scheme. There are three main attack models that describe the capabilities of an adversary to attack a cryptosystem (Wyseur 2009). First is the black-box model. This is a traditional attack model in which an adversary only has access to the functionality of a cryptosystem. In this way, it is difficult and time-consuming for adversaries to perform attacks. The second model is the gray-box model, which refers to a model that a leakage function is present. In such an attack context, the adversary can deploy side-channel cryptanalysis techniques. Due to the large variety of leakage functions, several gray-box models can be defined. Third is the white-box model, in which the adversary has total visibility into the software implementation of the cryptosystem and

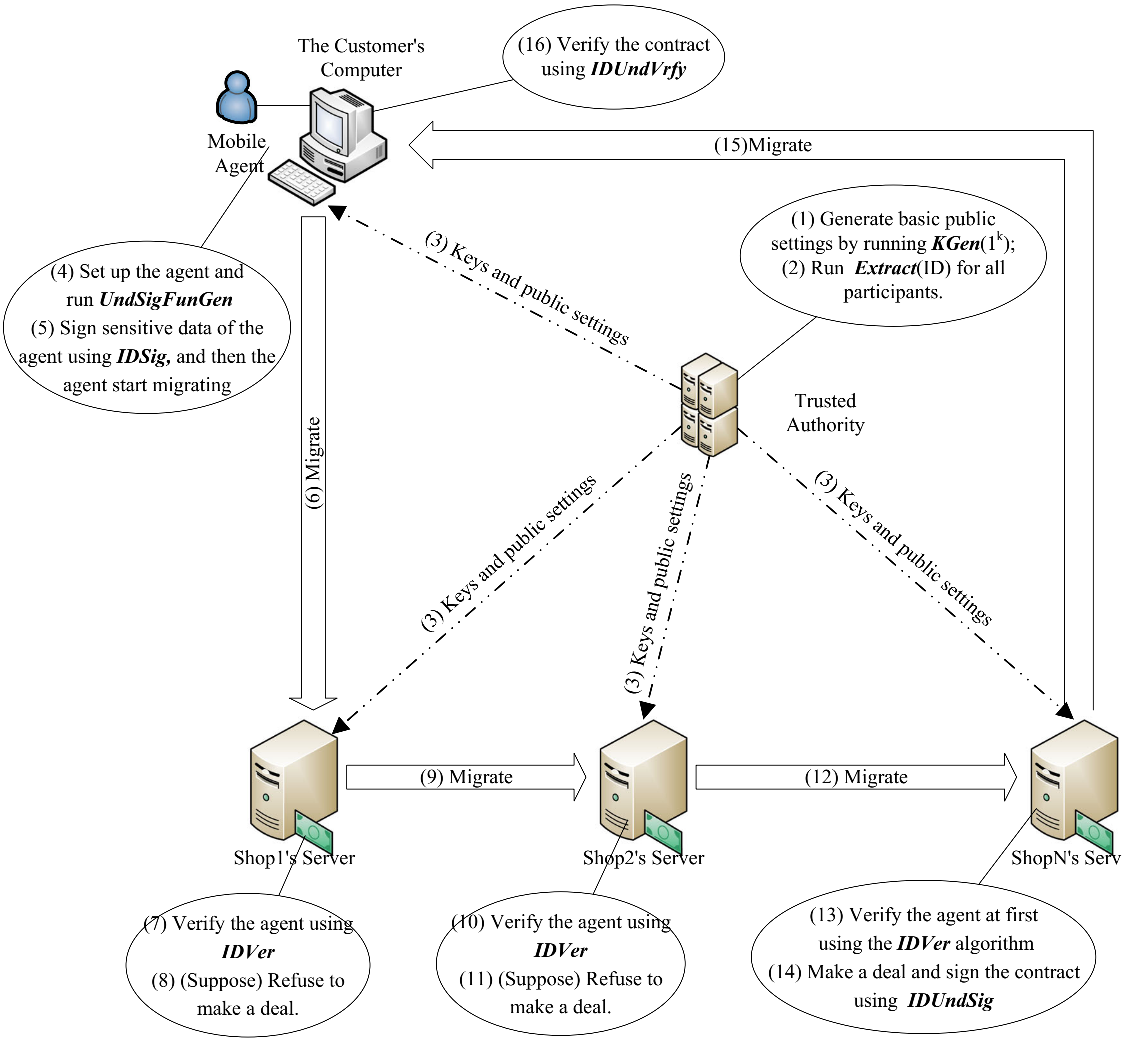

The Customer's Computer
(16) Verify the contract using IDUndVrfy
Mobile Agent
(15)Migrate
(1) Generate basic public settings by running KGen(1^k);
(2) Run Extract(ID) for all participants.
(3) Keys and public settings
(4) Set up the agent and run UndSigFunGen
(5) Sign sensitive data of the agent using IDSig, and then the agent start migrating
(6) Migrate
Trusted Authority
(3) Keys and public settings
(3) Keys and public settings
(3) Keys and public settings
(9) Migrate
(12) Migrate
Shop1's Server
Shop2's Server
ShopN's Server
(7) Verify the agent using IDVer
(8) (Suppose) Refuse to make a deal.
(10) Verify the agent using IDVer
(11) (Suppose) Refuse to make a deal.
(13) Verify the agent at first using the IDVer algorithm
(14) Make a deal and sign the contract using IDUndSig

Fig. 3 Usage of algorithms

full control over its execution platform. In other words, the implementation of the cryptosystem is running in a WBAC, as we described in Sect. 2. The white-box model can be considered the worst-case model. In contrast to gray-box models, it is impossible for an adversary not to comply with the model. The white-box model is used to analyze algorithms that are running in a non-trustable environment, that is, an environment in which applications are subject to attacks from the execution platform.

Traditionally, there are four subclasses of known-message attacks against digital signature schemes in black-box attack contexts (Pointcheval and Stern 1996, 2000): the plain known-message attack, the generic chosen-message attack, the oriented chosen-message attack, and the adaptively chosen-message attack (ACMA). In an ACMA, an adversary has knowledge of the public key of the signer and is able to ask the signer to sign any message that the adversary wants. The adversary can then adapt queries according to previous message–signature pairs. This is the most powerful attack type in black-box attack contexts.

Usually, EUF-ACMA is a sufficiently strict security notion for digital signature schemes in the black-box model. As to identity-based signature schemes, the selective identity attack should also be considered. Therefore, EUF-ACMIA is the most widely used security notion for identity-based digital signature schemes in which “I” stands for “identity.” But for white-box attack contexts, because an adversary may collect many implementations of $f_{Signed}()$ generated by the algorithm $UndSigFunGen$, we suppose that the adversary can call the $UndSigFunGen$ algorithm adaptively. Hence, we give the EUF-ACMIUA (existential universal forgery-adaptively chosen message, identity and undetachable signing function attack) as a security notion for identity-based undetachable digital signature schemes where “U” stands for “undetachable signature function.”

For an adversary $\mathcal{A} =< \mathcal{A}_1, \mathcal{A}_2 >$, let

$$
\begin{aligned}
&Adv_{\mathcal{A}_1}(k)\\
&= \Pr\left[\begin{array}{l}
\Omega \leftarrow KGen\left(1^k\right)\\
(ID, msg, \Sigma) \leftarrow \mathcal{A}_1^{\begin{array}{l}O^{IDSig}(\cdot),\\ O^{UndSigFunGen}(\cdot),\\ O^{Extract}(\cdot)\end{array}}(\Omega) :\\
\quad 1 = IDVer\,(ID, msg, \Sigma)\\
\quad \wedge (ID, REQ) \notin L_{UndSigFunGen}\\
\quad \wedge (ID, msg) \notin L_{IDSig}\\
\quad \wedge ID \notin L_{Extract}
\end{array}\right]
\end{aligned}
\tag{3}
$$

where L_{IDSig}, $L_{UndSigFunGen}$, and $L_{Extract}$ are the query lists coming from the signing oracle $O^{IDSig}(\cdot)$, the undetachable signing oracle $O^{REQ}_{IDUndSig}(\cdot)$, the undetachable signature function generation oracle $O^{UndSigFunGen}(\cdot)$, and the extract oracle $O^{Extract}(\cdot)$, respectively, during the attack. Also let

$$
\begin{aligned}
&Adv_{\mathcal{A}_2}(k)\\
&= \Pr\left[\begin{array}{l}
\Omega \leftarrow KGen\left(1^k\right)\\
(ID, REQ, msg, \Sigma) \leftarrow \mathcal{A}_2^{\begin{array}{l}O^{IDSig}(\cdot),\\ O^{UndSigFunGen}(\cdot),\\ O^{Extract}(\cdot)\end{array}}(\Omega) :\\
1 = IDUndVrfy\,(ID, REQ, msg, \Sigma)\\
\;\wedge (ID, REQ) \notin T_{UndSigFunGen}\\
\;\wedge (ID, REQ) \notin T_{IDSig} \wedge ID \notin T_{Extract}
\end{array}\right]
\end{aligned}
\tag{4}
$$

where T_{IDSig}, $T_{UndSigFunGen}$, and $T_{Extract}$ are the query lists coming from the signing oracle $O^{IDSig}(\cdot)$, the undetachable signature function generation oracle $O^{UndSigFunGen}(\cdot)$, and the extract oracle $O^{Extract}(\cdot)$, respectively, during the attack.

We define the advantage of the adversary $\mathcal{A}$ as follows:

$$Adv_{\mathcal{A}}(k) = Adv_{\mathcal{A}_1}(k) + Adv_{\mathcal{A}_2}(k) \tag{5}$$

We use PPT to denote probabilistic, polynomial-time Turing machines and $Negl$ to denote the family of all negligible functions. An identity-based undetachable digital signature scheme is EUF-ACUIMA-secure if:

$$
\begin{aligned}
&\forall \mathcal{A} \in PPT, \exists negl\,(k) \in Negl\,(k),\\
&Adv_{\mathcal{A}}\,(k) \leq negl\,(k)
\end{aligned}
\tag{6}
$$

4 A concrete scheme

This section proposes an identity-based undetachable digital signature scheme that is EUF-ACUIMA-secure. The correctness and security of the proposed scheme are proven, and the time complexity is analyzed. The proposed scheme uses common settings and a key generation algorithm similar to many other identity-based security schemes based on bilinear pairings, such as in Boneh and Franklin (2003); Steinwandt and Corona (2012); Tariq et al. (2014). Furthermore, it uses an identity-based digital signature scheme given by Gopal et al. (2013) as a base scheme. But the crucial components of the proposed scheme, especially the $UndSigFunGen$ algorithm, the $IDUndsig$ algorithm, and the $IDUndVrfy$ algorithm, are new.

4.1 Security and computational assumptions

Suppose that G is an additive group. Three well-known mathematical problems are defined as follows.

Discrete logarithm problem (DLP) on elliptic curves: given two group elements P and Q, output an integer n, such that (7) is satisfied if such an integer exists:

$$Q = nP \tag{7}$$

Decision Diffie–Hellman Problem (DDHP): For $\{a, b, c\} \subseteq Z_q^*$, given P, aP, bP, cP, decide whether:

$$c \equiv ab(\mathrm{mod}q) \tag{8}$$

Computational Diffie–Hellman Problem (CDHP): For $\{a, b\} \subseteq Z_q^*$, given P, aP, bP, output the value of abP without any knowledge about the value of either a or b.

In addition, a Gap Diffie–Hellman Group (GDHG) is a group for which DDHP is easy, but CDHP is hard.

We say that an algorithm (t, ε) breaks the CDH problem if the CDH problem can be solved in time t with a probability at least ε. The CDH problem is (t, ε)-hard if there is no algorithm that (t, ε)-breaks the CDH problem. Let k be the order of P and suppose that the running time and numbers of queries made by the adversary are bounded by polynomials in k. At present, for sufficiently large k, no PPT algorithm is known to be able to solve CDHP with a non-negligible advantage. That is, for any challenger $\mathcal{C} \in PPT$, let $Adv_{\mathcal{C}}(k)$ be the advantage of $\mathcal{C}$ in solving CDHP, there exists $negl_{\mathcal{C}}(k) \in Negl(k)$, such that $Adv_{\mathcal{C}}(k)$ is not larger than $negl_{\mathcal{C}}(k)$. The hardness is a reasonable assumption for the security proofs of our identity-based undetachable digital signature scheme. Furthermore, there should be a polynomial-time algorithm that can solve the DDHPs so that the verification algorithm of the proposed scheme can be performed efficiently. That is, the groups in the common key settings that are introduced in the next subsection are GDHGs.

4.2 Algorithms

Before the introduction of concrete algorithms, we list the frequently used symbols in Table 1.

Table 1 Symbols

Symbol	Description
$G_1,\ G_2$	Cyclic groups
P	The generator of G_1
q	$q = \|G_1\| = \|G_2\|$
1^k	A security parameter, $k \in \mathbb{N}$
P_{pub}	The master public key
$\widehat{e}$	The bilinear mapping
H_2	A hash mapping from $\{0, 1\}^*$ onto G_1
H_3	A hash mapping from $\{0, 1\}^* \times G_2$ onto Z_q^*
g	$g = \widehat{e}\left(P, P_{pub}\right) \in G_2$
s	The master secret key
ID_C	Customer C's identity
D_{ID}	ID's secret signing key
Q_{ID}	ID's public key, $Q_{ID} = H_2\,(ID)$
REQ_C	Customer C's requirement
f_{Signed}	An implementation of the identity-based undetachable signing function
f	The auxiliary function of f_{Signed}
$Msg\ (m)$	A message (typically a contract)
z	An undetachable signature
Σ	A normal (identity-based) signature

The proposed identity-based undetachable digital signature scheme consists of seven algorithms as follows:

Algorithm 1 $KGen\,(\cdot)$:

On input 1^k where $k \in \mathbb{N}$ is a security parameter, the algorithm outputs the common key settings $\Omega = (G_1, G_2, \widehat{e}(\cdot,\cdot), q, P, P_{pub}, g, H_2, H_3)$ and the masker key s.

In the common key settings, G_1 is a cyclic group generated by a generator P, whose order is a prime number q, and G_2 is a cyclic multiplicative group of the same order q. Suppose discrete logarithm problems in both G_1 and G_2 are hard. The mapping $\widehat{e} : G_1 \times G_1 \to G_2$ is a bilinear mapping that satisfies the following three conditions:

Bilinear: (9) and (10) or (11)

$$\widehat{e}(P_1 + P_2, Q) = \widehat{e}(P_1, Q)\widehat{e}(P_2, Q) \tag{9}$$

$$\widehat{e}(P, Q_1 + Q_2) = \widehat{e}(P, Q_1)\widehat{e}(P, Q_2) \tag{10}$$

$$\widehat{e}(aP, bQ) = \widehat{e}(P, Q)^{ab} \tag{11}$$

where $\{a, b\} \subseteq Z_q^*$.

Non-degenerate: There exists $P \in G_1$ and $Q \in G_1$ subject to (12).

$$\widehat{e}(P, Q) \neq 1 \tag{12}$$

Computability: There is an efficient algorithm to compute $\widehat{e}(P, Q)$ for all$\{P, Q\} \subseteq G_1$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps. Please refer to (Arène et al. 2011; Freeman and Satoh 2011; Lauter and Shang 2013; TaeChan et al. 2013) for further mathematical backgrounds.

Now some system parameters can be generated as follows: Let P be a generator of G_1, pick a random number $s \in Z_q^*$, then set $P_{pub} = sP$ and $g = \widehat{e}(P, P_{pub}) \in G_2$. Moreover, two secure hash functions are given in the common key settings: $H_2 : \{0, 1\}^* \to G_1$ and $H_3 : \{0, 1\}^* \times G_2 \to Z_q^*$. The implementation of these hash functions can be found in works such as (Farashahi et al. 2013; Icart 2009; Kawahara et al. 2011). Ω should be published to all participants by the trusted authority (TA).

We assume through this paper that CDHP and DLP are intractable in the common key settings, which means there is no polynomial-time algorithm to solve CDHP or DLP with non-negligible probability. When the DDHP is easy, but the CDHP is hard on the group G_1, G_1 is called a Gap Diffie–Hellman (GDH) group. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite fields, and the bilinear parings can be derived from the Weil or Tate pairing $e : G_1 \times G_1 \to G_2$. Our scheme can be built on any GDH group. More mathematical background can be found in Boneh and Franklin (2003).

Algorithm 2 *Extract* When an identity ID is provided as input, the algorithm outputs the private key $D_{ID} = sQ_{ID}$ where $Q_{ID} = H_2(ID)$.

Remark 1 For an identity ID, $Q_{ID} = H_2(ID)$ plays the role of the associated public key. The private key should be secretly sent via a secure channel.

Remark 2 The first two algorithms are similar to corresponding algorithms in other identity-based signature schemes; in particular, they are the same as the two corresponding algorithms in Gopal et al. (2013), except for some differences in description.

Algorithm 3 $UndSigFunGen$

Input $REQ\_C, Q_{ID_C}, D_{ID_C}$

$$r \overset{r}{\leftarrow} Z_q^*;\ U \leftarrow g^r;\ h \leftarrow H_3(REQ\_C, U)$$

$$V \leftarrow D_{ID_C} + rhP_{pub};\ t \overset{r}{\leftarrow} Z_q^*;\ A_1 \leftarrow g^t;\ A_2 \leftarrow tP_{pub}$$

Output the function $f_{Signed}(\cdot)$ where:

$$f_{Signed}(x) = \langle\langle U, V, A_1\rangle, V + xA_2\rangle \tag{13}$$

Remark 3 U and V are generated using the technique that is introduced in Gopal et al. (2013).

Algorithm 4 $IDUndSig$

```
Input $CONTRACT$

$x \leftarrow H_3(CONTRACT, A_1)$

$z \leftarrow f_{Signed}(x) = \langle\langle U, V, A_1\rangle, V + xA_2\rangle$

Output $z$
```

Algorithm 5 $IDUndVrfy$

```
Input $CONTRACT, z = \langle\langle U, V, A_1\rangle, B\rangle$

(1) Extract $ID_C$, $REQ\_C$ and $BID\_S$ from the string $CONTRACT$. If $BID\_S$ does not satisfy $REQ\_C$, output 0 and terminate the algorithm, else go to (2).
(2) Extract $< U, V >$ from $z$.
(3) Compute:

    $$Equal\left(\widehat{e}(P, V), \widehat{e}\left(P_{pub}, H_2(ID_C)\right) U^{H_3(REQ\_C,U)}\right) \tag{14}$$

    If the output is 1, go to (4); Else, output 0 and terminate the algorithm.
(4) $x \leftarrow H_3(CONTRACT, A_1)$
(5) $B \leftarrow V + xA_2$, $Q_{ID_C} \leftarrow H_2(ID_C)$
(6) Compute a bit value $b$ as in (15) and output the value of $b$.

    $$b = Equal\left(\widehat{e}(P, B), \widehat{e}(P_{pub}, Q_{ID_C})U^{H_3(REQ\_C,U)}A_1^x\right) \tag{15}$$
```

Remark 4 $Equal : G_2 \times G_2 \rightarrow \{0, 1\}$ outputs 1 when the two inputs are equal and outputs 0 if not.

Remark 5 Note that the signing algorithm and the verification algorithm of our scheme only work on the second part of a message $m =< m_1, m_2 >$, i.e., only is signed and verified. Security notions about Algorithms 6 and 7 should only take the second part of a message (m_2) in account. We modify the signing algorithm and verification algorithm of (Gopal et al. 2013) to get the following two algorithms.

Algorithm 6 *IDSig*

```
Input $m =< m_1, m_2 >$

$t \leftarrow^r Z_q^*$; $A_1 \leftarrow g^t$; $A_2 \leftarrow tP_{pub}$

$y_1 \leftarrow m_1$; $y_2 \leftarrow H_3(m_2, A_1)$; $y \leftarrow< y_1, y_2 >$

Output $Sig(y)$, where the function $Sig(\cdot)$ is defined in (16).

$$Sig(y) = \left\langle\langle y_1, A_1\rangle, D_{ID_C} + y_2A_2\right\rangle \tag{16}$$
```

Algorithm 7 *IDVer*

```
Input $\Sigma =< \Sigma_1, \Sigma_2 >, m =< m_1, m_2 >$
Parse $\Sigma_1 = (y_1, A_1)$
Output $Equal\left(\widehat{e}(P, \Sigma_2), \widehat{e}\left(P_{pub}, H_2(ID_C)\right) A_1^{H_3(m_2,A_1)}\right)$
```

4.3 Correctness

In this subsection, we first prove the correctness of the verification algorithm. Suppose that $z = \langle\langle U, V, A_1\rangle, B\rangle$ is a valid identity-based undetachable signature on *CONTRACT* = $REQ\_C||ID_S||BID\_S||T_{BID\_S}$ signed by a customer whose identifier is ID_C with a restriction of requirement REQ_C, we have the following two lemmas.

Lemma 1 $\widehat{e}(P, V) = \widehat{e}\left(P_{pub}, H_2(ID_C)\right) U^{H_3(REQ\_C,U)}$

Proof

$$\begin{aligned}
&\widehat{e}\left(P_{pub}, H_2(ID_C)\right) U^{H_3(REQ\_C,U)}\\
&= \widehat{e}\left(P_{pub}, H_2(ID_C)\right) g^{r\cdot H_3(REQ\_C,U)}\\
&= \widehat{e}(sP, H_2(ID_C)) g^{r\cdot H_3(REQ\_C,U)}\\
&= \widehat{e}\left(P, D_{ID_C}\right) g^{r\cdot H_3(REQ\_C,U)}\\
&= \widehat{e}\left(P, D_{ID_C}\right) g^{r\cdot h}\\
&= \widehat{e}\left(P, D_{ID_C}\right) \widehat{e}\left(P, P_{pub}\right)^{r\cdot h}\\
&= \widehat{e}\left(P, D_{ID_C}\right) \widehat{e}\left(P, rhP_{pub}\right)\\
&= \widehat{e}\left(P, D_{ID_C} + rhP_{pub}\right) = \widehat{e}(P, V)
\end{aligned}$$

This ends the proof. □

Lemma 2 $\widehat{e}(P, B) = \widehat{e}(P_{pub}, Q_{ID_C})U^{H_3(REQ\_C,U)}A_1^{\overline{x}}$ *where* $\overline{x} = H_3(CONTRACT, U)$, $Q_{ID_C} = H_2(ID_C)$ *and* $B = V + \overline{x}tP_{pub}$.

Proof

$$\begin{aligned}
&\widehat{e}\left(P_{pub}, Q_{ID_C}\right) U^{H_3(REQ\_C,U)} A_1^{\overline{x}}\\
&= \widehat{e}\left(P_{pub}, Q_{ID_C}\right) g^{r\cdot H_3(REQ\_C,U)} g^{t\cdot\overline{x}}\\
&= \widehat{e}\left(P_{pub}, Q_{ID_C}\right) \widehat{e}\left(P_{pub}, P\right)^{r\cdot H_3(REQ\_C,U)} \widehat{e}\left(P_{pub}, P\right)^{t\cdot\overline{x}}\\
&= \widehat{e}\left(P_{pub}, Q_{ID_C} + rH_3(REQ\_C, U)P + t\overline{x}P\right)\\
&= \widehat{e}\left(P, sQ_{ID_C} + srH_3(REQ\_C, U)P + st\overline{x}P\right)\\
&= \widehat{e}\left(P, D_{ID_C} + rH_3(REQ\_C, U)P_{pub} + t\overline{x}P_{pub}\right)\\
&= \widehat{e}\left(P, V + t\overline{x}P_{pub}\right) = \widehat{e}(P, B)
\end{aligned}$$

This ends the proof. □

Based on Lemmas 1 and 2, we have the following proposition.

Proposition 1 *If* $z = \left\langle\langle K_1, K_2, R'\rangle, B\right\rangle$ *is a valid identity-based undetachable signature on the message CONTRACT* = *REQ_C* || ID_S || *BID_S* || T_{BID_S} *which is signed by a customer whose identifier is* ID_C *with a restriction of requirement REQ_C, and it is obviously that* 1 = *IDUndVrfy*(*z*, *CONTACT*).

Proof Because z is a valid identity-based undetachable signature, it is clear that BID_S must satisfy REQ_C.

Furthermore, according to on Lemmas 1 and 2, the following two equations hold:

$$1 = Equal \left(\begin{array}{l} e\left(P, V\right), e\left(P_{pub}, H_2\left(ID_C\right)\right) \\ U^{H_3(REQ\_C,U)} \end{array} \right) \tag{17}$$

$$1 = Equal \left(\begin{array}{l} e\left(P, B\right), e\left(P_{pub}, H_2\left(ID_C\right)\right) \\ U^{H_3(REQ\_C,U)} A_1^x \end{array} \right) \tag{18}$$

Hence, the output of $IDUndVrfy\left(z, CONTACT\right)$ is 1. This ends the proof. □

The following proposition shows that the proposed scheme satisfies Eq. (1) in Sect. 2.

Proposition 2 *Let*

$$< y_1, y_2 >= y = f(x) = \left\langle \begin{array}{l} (U, V), t^{-1} r H_3 \\ (REQ\_C, U) + x \end{array} \right\rangle \tag{19}$$

for the function $Sig(y)$ and $f_{Signed}(x)$ that are defined in (16) and (13), respectively; in this case, the equation $f_{Signed}(x) = (Sig \circ f)(x)$ holds.

Proof

$$\begin{aligned} & f_{Signed}(x) \\ &= \langle\langle U, V, A_1\rangle, V + xA_2\rangle \\ &= \left\langle\langle U, V, A_1\rangle, D_{ID_C} + rH_3\left(REQ\_C, U\right) P_{\ pub} + xA_2\right\rangle \\ &= \left\langle\langle U, V, A_1\rangle, D_{ID_C} + \left(t^{-1} rH_3\left(REQ\_C, U\right) + x\right) A_2\right\rangle \\ &= \left\langle\langle y_1, A_1\rangle, D_{ID_C} + y_2 A_2\right\rangle \\ &= \left(Sig \circ f\right)(x) \end{aligned}$$

This ends the proof. □

4.4 Proof of security

In this section, we provide security proof of the proposed identity-based undetachable signature scheme.

Lemma 3 *Existential universal forgery against $IDVer$ that is given by Algorithm 7 can be reducted to solve the CDH problem in .G_1.*

Proof Because the signing algorithm $IDSig$ and the verification algorithm $IDVer$ of our scheme only work on the second part of a message $m =< m_1, m_2 >$, only m_2 is signed and verified. As we stated in Remark 5, we only take the integrality of the second part of a message (m_2) in account. The signature generated on $m =< m_1, m_2 >$ using $IDSig$ of our scheme can be easily reduced to a signature on m_2 that is generated using the signing algorithm of (Gopal et al. 2013). Hence, according to theorem 1 of (Gopal et al. 2013), existential universal forgery against $IDVer$ can be reducted to solving the CDH problem in G_1. □

Lemma 4 *Existential universal forgery against $IDUndVrfy$ that is given by Algorithm 5 can be reducted to solve the CDH problem in G_1.*

Proof First, we construct a security game as shown in Fig. 3. In this security game, there are three players: $\mathcal{A}_2$, $\mathcal{B}$ and Sim. $\mathcal{A}_2$ is a white-box attacker that can directly access implementations of the undetachable signing algorithm. The message is in the form of $Msg = (m_1, m_2)$. The challenger $\mathcal{B}$ plays between $\mathcal{A}_2$ and Sim. $\mathcal{A}_2$ is able to make queries $O^{Extract}(\cdot)$, $O^{UndSigFunGen}(\cdot, \cdot)$, $O^{IDSig}(\cdot, \cdot)$, $O^{H_3}(\cdot)$, and $O^{H_2}(\cdot)$. $\mathcal{B}$ is responsible for answering these queries with the help of Sim. Sim should answer queries $Extract(\cdot)$, $S(\cdot)$, $H_3(\cdot)$, and $H_2(\cdot)$, from $\mathcal{B}$, where $S(\cdot)$ is the standard identity-based signing algorithm introduced in (Gopal et al. 2013). □

As shown in Fig. 4, there are two algorithms ψ and ϕ which are used to help $\mathcal{B}$ plays with $\mathcal{A}_2$.

ψ is an algorithm of $\mathcal{B}$ that works as follows.

Input ID, REQ and $< U, V >\in G_2 \times G_1$

$$< U, V >\leftarrow S(ID, REQ)$$
$$t \leftarrow^r Z_q^*;\ A_1 \leftarrow g^t;\ A_2 \leftarrow tP_{pub}$$

Output the function $f_{Signed}(\cdot)$ where:

$$f_{Signed}(x) = \langle\langle U, V, A_1\rangle, V + xA_2\rangle$$

ϕ is an algorithm of $\mathcal{B}$ that works as follows.

Input ID, $Msg = (m_1, m_2)$

$$< \alpha, \beta >\leftarrow S(ID, m_2)$$

Output the signature $\langle < m_1, \alpha >, \beta\rangle$

Let c_{G_1} be the time required to compute a scalar multiplication in G_1 and an inversion in Z_q^*, and let c_{G_1} be the time required to compute a pairing. Let c_ψ be the additional time required to compute "$t \leftarrow^r Z_q^*$, $A_1 \leftarrow g^t$, $A_2 \leftarrow tP_{pub}$."

Suppose that $\mathcal{A}_2$ can win the game that queries $O^{Extract}(\cdot)$, $O^{UndSigFunGen}(\cdot, \cdot)$, $O^{IDSig}(\cdot, \cdot)$, $O^{H_3}(\cdot)$ and $O^{H_2}(\cdot)$ at most q_K, q_U,q_S, q_{O_3} and q_{O_2} times, respectively, and has a running time of T_0 and an advantage ε_0, then $\mathcal{B}$ can break the scheme with queries $Extract(\cdot)$, $S(\cdot)$, $H_3(\cdot)$, and $H_2(\cdot)$ at most q_K, $q_S + q_U$, q_{O_3} and q_{O_2} times, respectively, and has a running time of $T = T_0 + c_\psi q_U$ and an advantage $\varepsilon = \varepsilon_0$. By theorem 1 of (Gopal et al. 2013), suppose that the CDH problem is (T', ε') hard, then within an attack time of $T \leq T' - c_{G_1} c_{G_2}(q_{O_3} + q_E + 3q_S + 5)$, no adversary can win the ACIMA-EUF game at a probability $\varepsilon \geq e \cdot (q_E + 1) \cdot \varepsilon'$. Thus, we have that within an attack time of $T_0 \leq T' - c_{G_1} c_{G_2}(q_{O_3} + q_E + 3q_S + 5) - c_\psi q_U$, $\mathcal{A}_2$ cannot win this game at a probability $\varepsilon_0 \geq e \cdot (q_E + 1) \cdot \varepsilon'$. This ends the proof.

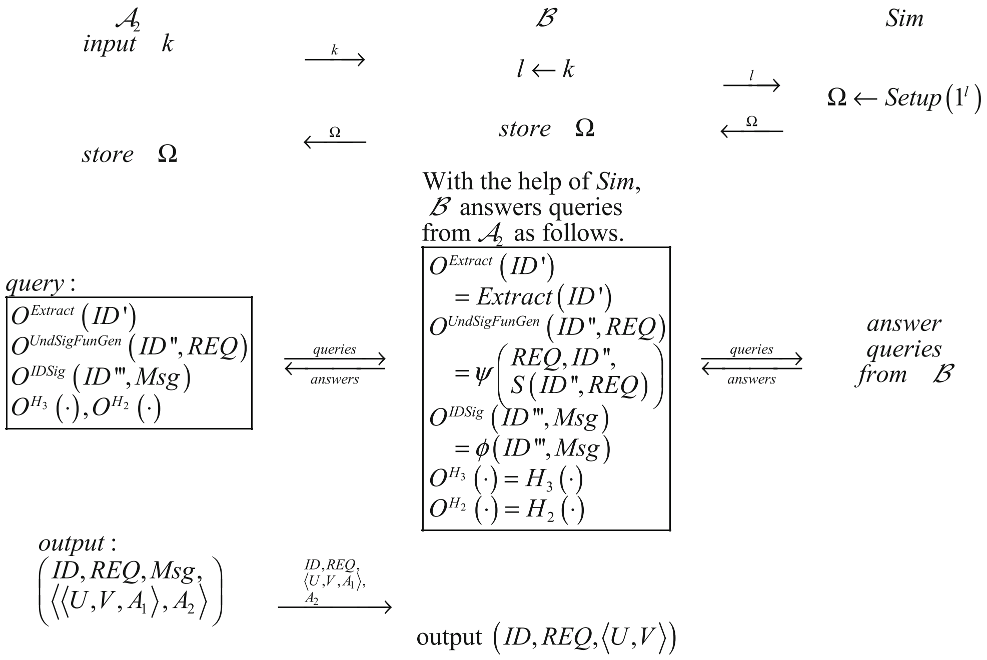

$\mathcal{A}_2$
$\mathcal{B}$
Sim
$input \quad k$
k
$l \leftarrow k$
l
$\Omega \leftarrow Setup(1^l)$
Ω
Ω
$store \quad \Omega$
$store \quad \Omega$
With the help of Sim, $\mathcal{B}$ answers queries from $\mathcal{A}_2$ as follows.
$query:$
$O^{Extract}(ID')$
$O^{UndSigFunGen}(ID'', REQ)$
$O^{IDSig}(ID''', Msg)$
$O^{H_3}(\cdot), O^{H_2}(\cdot)$
queries
answers
$O^{Extract}(ID') = Extract(ID')$
$O^{UndSigFunGen}(ID'', REQ) = \psi\begin{pmatrix} REQ, ID'', \\ S(ID'', REQ) \end{pmatrix}$
$O^{IDSig}(ID''', Msg) = \phi(ID''', Msg)$
$O^{H_3}(\cdot) = H_3(\cdot)$
$O^{H_2}(\cdot) = H_2(\cdot)$
queries
answers
answer queries from $\mathcal{B}$
$output:$
$\begin{pmatrix} ID, REQ, Msg, \\ \langle\langle U, V, A_1\rangle, A_2\rangle \end{pmatrix}$
$ID, REQ, \langle U, V, A_1\rangle, A_2$
output $(ID, REQ, \langle U, V\rangle)$

Fig. 4 The security game

Based on Lemmas 3 and 4, we have the following proposition.

Proposition 3 *The proposed scheme is EUF-ACUIMA secure.*

Proof We use PPT to denote probabilistic, polynomial-time Turing machines and $Negl$ to denote the family of all negligible functions. Since we assume the CDH is hard, according to Lemma 7, for any adversary $\mathcal{A}_1 \in PPT$, if the adversary can acquire the advantage that is defined by (3), then $\exists negl_1(k) \in Negl(k)$, $Adv_{\mathcal{A}_1}(k) \leq negl_1(k)$, where k is the order of P. Similarly, according to Lemma 8, for any adversary $\mathcal{A}_2 \in PPT$, if the adversary can acquire the advantage that is defined by (4), then $\exists negl_2(k) \in Negl(k)$, $Adv_{\mathcal{A}_2}(k) \leq negl_2(k)$, where k is the order of P. Therefore, we have:

$$\begin{aligned} &Adv_{\mathcal{A}_1}(k) + Adv_{\mathcal{A}_2}(k) \leq \\ &(negl_1(k) + negl_2(k)) \in Negl(k) \end{aligned} \tag{20}$$

This ends the proof. □

4.5 Complexity analysis and experimental results

The mathematical operations used in this scheme are mainly modular multiplication $\langle Z_q^*, Z_q^*\rangle \rightarrow Z_q^*$, scalar multiplication $\langle Z_q^*, G_1\rangle \rightarrow G_1$, addition $\langle G_1, G_1\rangle \rightarrow G_1$, bilinear map $\widehat{e} = (G_1 \times G_1 \rightarrow G_2)$, multiplication $G_2 \times G_2 \rightarrow G_2$, exponentiation $\langle Z_q^*, G_2\rangle \rightarrow G_2$ and the two hash functions H_2, H_3. All these operations are polynomial bounded operations and can be computed effectively. In Table 2 we give the number of operations required for algorithms in the proposed scheme.

Table 2 The number of operations required for the algorithms in this scheme

Operation	Algorithm					
	2	3	4	5	6	7
$\boldsymbol{H}_2$	1	0	0	1	0	1
$\boldsymbol{H}_3$	0	1	1	2	1	1
G_1						
Scalar multiplication	1	2	1	1	2	0
Point addition	0	1	1	1	1	0
Bilinear map	0	0	0	4	0	2
G_2						
Multiplication	0	0	0	3	0	1
Exponentiation	0	2	0	3	1	1
Z^*						
Modular multiplication	0	1	0	0	0	0
Random selection	0	2	0	0	1	0

The algorithms have been implemented in Java, which has been used instead of C/C++ because a large number of mobile agent platforms are developed in Java, although C/C++ is

Table 3 The configurations of testing platforms

Platform	CPU	RAM (GB)	OS	JDK
PC1	Intel i5 2Cores, 1.7 GHz	4	Win7	7.0
PC2	Intel i7 2Cores, 1.9 GHz	8	Win8	7.0
Server	Intel E5 6Cores * 2, 2.5 GHz	96	WinServ 2008	7.0

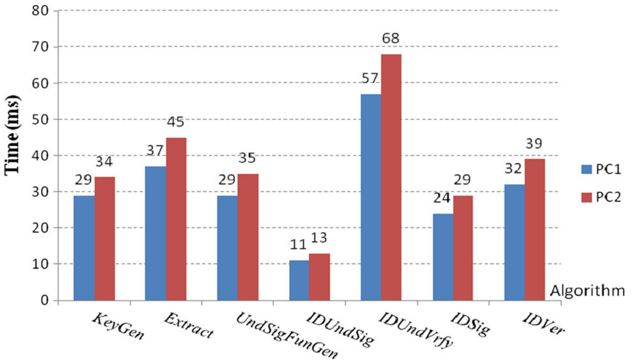


Fig. 5 Running time (ms) on PC1 and PC2 for each algorithm in the proposed scheme

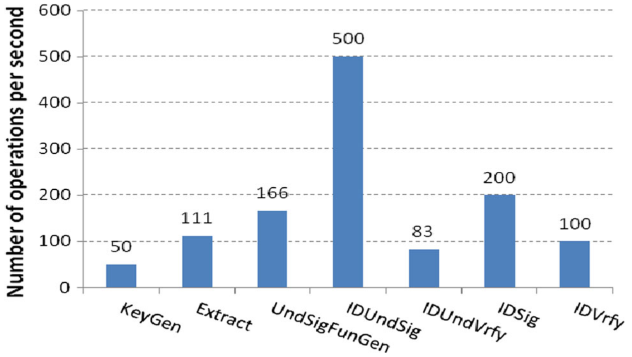


Fig. 6 Number of operations per second on the server for each algorithm in the proposed scheme

known to be more efficient. JPBC, an open-source Java Pairing-Based Cryptography Library (De Caro and Iovino 2011), is used in our implementation. The configurations of the testing platforms are listed in Table 3, and the experimental results are shown in Figs. 5 and 6.

When the computing platform is a PC, we focus on the speed of algorithms. In Fig. 5, we show the speed of the algorithms on two different portable computer in single-thread mode. When the computing platform is a server, the most important index of the performance is that how many transactions can be processed in a short time span (e.g., a second). Hence, Fig. 6 shows the number of operations of each algorithm on a PC Server in multi-threads mode. The experimental results indicate that the algorithms in the proposed scheme are quite efficient.

5 Comparison with related works

In this section, the proposed scheme is compared with those in the relative works through both theoretical analysis and experimental tests.

In theoretical aspects, the differences between the proposed scheme and those in relative works are shown in Table 4.

Compared with other undetachable signature schemes, the most significant feature of the proposed scheme is that it is identity-based. Moreover, the scheme has a formal security definition and a strict proof of security, which makes the scheme more complete.

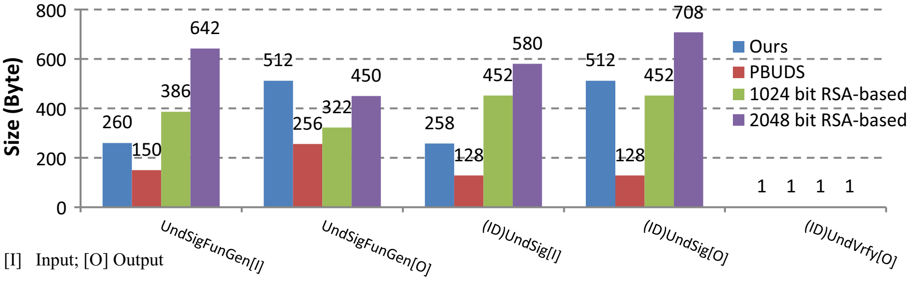
Table 4 shows that the pairing-based undetachable digital signature (thereafter PBUDS) scheme in (Shi et al. 2004b) is based on the same security assumption, i.e., the Computation Diffie–Hellman Problem on Gap Diffie–Hellman groups are computational infeasible when the security parameters are sufficiently large. It is convenient to compare the PBUDS scheme with the proposed scheme because we can use the same base cryptosystem and security parameters in analysis and testing.

Additionally, we also compare the proposed scheme with the first and most classical undetachable digital signature schemes, that is, Kotzanikolaou et al.'s scheme (2000). The scheme is based on the RSA cryptosystem, which is distinct from the pairing-based cryptosystem that is used in this paper. The main security parameter of the scheme, i.e., the length of modular, is setup to 1024 and 2048 bits, because the security strength of our scheme is between those of RSA-1024 and RSA-2048.

Three algorithms ($UndSigFunGen$, $UndSig$ and $UndVrfy$) are selected to compare on the size of input and output. As shown in Fig. 7, the size of input/output of our algorithms are larger than those of the PBUDS scheme in most cases. In addition, the sizes of input/output of our algorithms are comparable with those of the 1024 and 2048 bit RSA-based schemes. However, the input size of the $IDUndVrfy$ algorithm is much smaller than the input of $UndVrfy$ algorithm of the PBUDS scheme and those of the 1024 and 2048 bit RSA-based schemes, which hinges on the size of the customer's certification. A comparison on the input of $IDUndVrfy$ in the proposed scheme and $UndVrfy$ in the PBUDS scheme, as well as in the 1024 and 2048 bit RSA-based schemes is shown in Fig. 8. With the increment of the certification size, the input size of the $UndVrfy$ algorithm of the other schemes is linearly increased. However, the size of the $IDUndVrfy$ algorithm keeps constant because all of the algorithms in the proposed scheme are independent on

Table 4 A theoretical comparison of the proposed scheme with other undetachable signature schemes

References.	Computational infeasible problem(s)	identity-based	Other security features	Strict security proof
(Kotzanikolaou et al. 2000)	Factorization of a big integer	No	No	No
(Shi et al. 2004b)	Computational Diffie–Hellman Problem	No	No	No
(Lee et al. 2001)	Factorization of big integer	No	No	No
(Han et al. 2005)	q-Strong Diffie–Hellman Problem	No	No	No
(Shi et al. 2004a)	Discrete logarithm on elliptic curves	No	No	No
(Shi and Xiong 2013)	Factorization of a big integer and discrete logarithm on conic curves	No	Threshold	No
(Shi et al. 2015)	Computation Diffie–Hellman Problem	No	Forward-secure	Yes
Ours	Computation Diffie–Hellman Problem	Yes	No	Yes



[I] Input; [O] Output

Fig. 7 A comparison on the size (byte) of input/output of the three selected algorithms in the proposed scheme and that of the corresponding algorithms in the 1024 and 2048 bit RSA-based schemes, and the PBUDS scheme

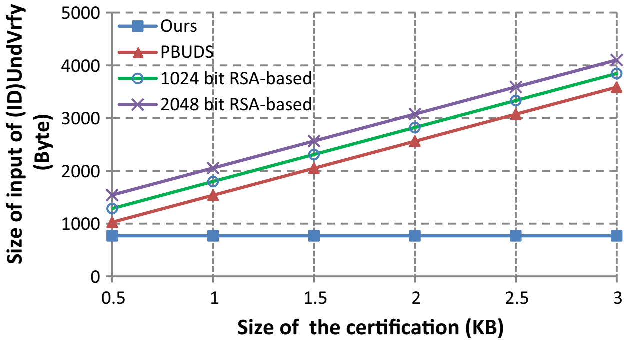


Fig. 8 A comparison on the input size of the proposed IDUndVer algorithm, and those of the UndVer algorithm of the 1024 and 2048 bit RSA-based schemes, and the PBUDS scheme

the size of a certification. Furthermore, we compared the total input and output size of the three algorithms with the increment of certification size in the proposed scheme and those of the PBUDS scheme, as well as those of the 1024 and 2048 bit RSA-based schemes. It is shown in Fig. 9 that the overall input and output size in the proposed scheme is remarkably smaller than that of the PBUDS scheme at certain size of the certification (around 1.5KB), and the size is always smaller than those of the 1024 and 2048 bit RSA-based schemes,

According to the experimental results in Fig. 10a the algorithms of the proposed scheme are more efficient than those of the PBUDS scheme generally. The overall performance is improved at the cost of slightly lower efficiency from the IDUndSig algorithm. According to the experimental results in Fig. 10b, the algorithms of the proposed scheme are slower than those of RSA-based scheme. However, Kotzanikolaou et al.'s RSA-based scheme is not provable secure, and the scheme does not support the strong version of RSA-based signature (i.e., as a probabilistic signature scheme).

According to Dodis et al. (2003), an identity-based signature scheme implies a key-insulated scheme. Therefore, the proposed scheme can also be used as a key-insulated undetachable signature scheme, which enables mobile agents to generate undetachable digital signatures on remote hosts with the key-insulated property of the original signer's signing key. The only comparable scheme with the key-insulated undetachable signature scheme is the forward-secure undetachable digital signature (thereafter FSUDS) scheme in (Shi et al. 2015) because both of the schemes have the security property of supporting key evolvement.

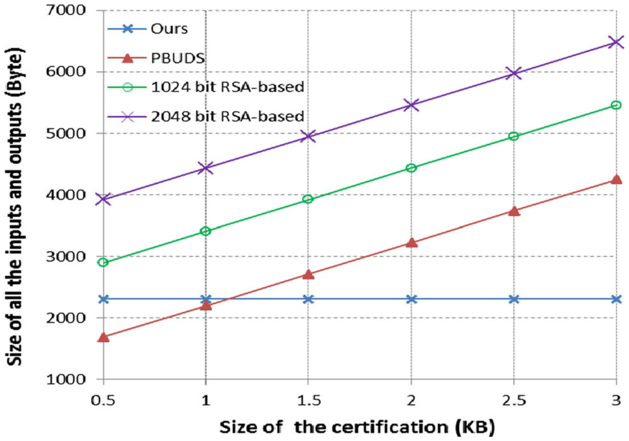


Fig. 9 A comparison on the overall input size of the three proposed algorithms, and those of the 1024 and 2048 bit RSA-based schemes, and the PBUDS scheme

Therefore, we compare the performance of the key-insulated scheme with the forward-secure scheme in Figs. 11 and 12. As shown in Fig. 11, among the algorithms, the size of input/output of the proposed algorithms is only 5% of those of the FSUDS scheme at the best case. As for the running time of the algorithms, as illustrated in Fig. 12, the maximal reduced time of the proposed algorithms is nearly 95% of that of the algorithms of the FSUDS scheme.

6 Conclusions

Compared with traditional computing models (e.g., the client/server model), mobile agent technology has several significant advantages for electronic commerce and other applications. However, because these agents may operate in WBACs on potentially malicious the hosts, a glaring threat is

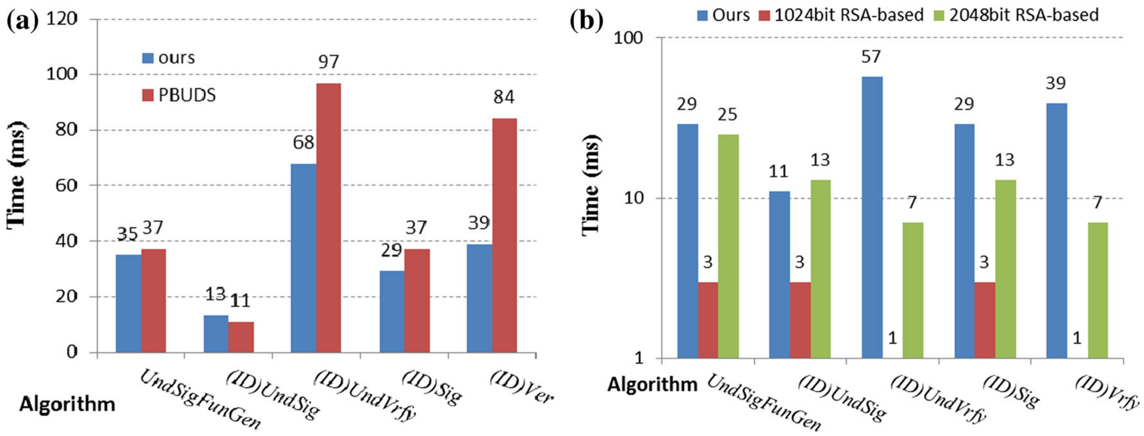


Fig. 10 A comparison on the running time (ms) of the algorithms in the proposed scheme and the corresponding algorithms of the PBUDS scheme, and the 1024 and 2048 bit RSA-based schemes, **a** compared with PBUDS, **b** Compared with RSA-based schemes

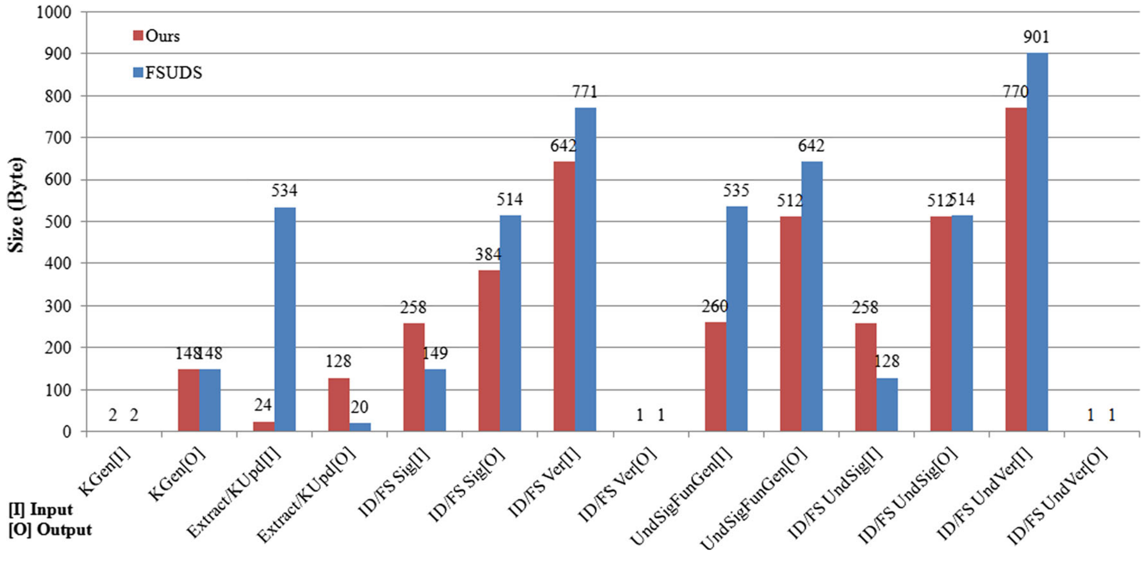


Fig. 11 Comparison on the size of input/output of the proposed algorithms with that of the corresponding algorithms of the FSUDS scheme

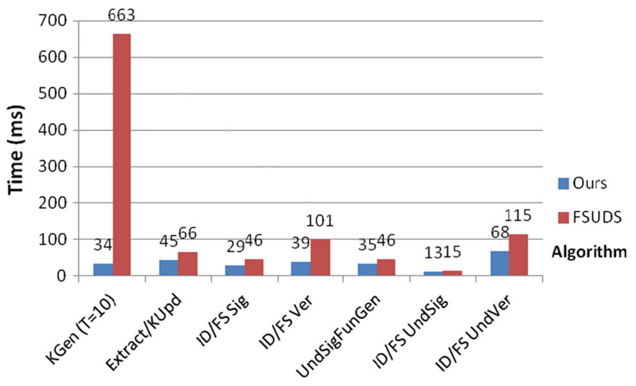


Fig. 12 Comparison on running time of the proposed algorithms with that of the corresponding algorithms of the FSUDS scheme

that malicious hosts might endanger passing agents. Therefore, these advantages cannot be reached without appropriate security countermeasures to guarantee that business data are well protected and business partners can work together with integrity.

In this paper, we proposed the idea of identity-based undetachable digital signatures so that mobile agents can perform identity-based signing operations on behalf of the original signers securely, even on malicious hosts. We provided a formal definition of identity-based undetachable digital signature schemes. Then, we gave the security notions of identity-based undetachable digital signature schemes as a theoretical basis. We proposed a concrete scheme with provable security for secure mobile agents in electronic commerce. The scheme is built on bilinear pairings, and its security depends on the hardness of solving CDH problems on GDH groups. An implementation of the proposed undetachable signature algorithm can securely migrate with mobile agents from one host to another without the risk that the signing key will be compromised or the signing algorithm might be misused. Moreover, because this scheme is identity-based, verification of the signatures generated by mobile agents does not require either communication with the CA or a certification of the original signer. Therefore, the costs of verification and even the dependence on a stable network connection are reduced.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Nos. 61772371, 61702372, 61202382, 61503286) and the Fundamental Research Funds for the Central Universities.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Aloui A, Zerdoumi O, Kazar O (2012) Architecture for mobile business based on mobile agent. In: 2012 International conference on paper presented at the multimedia computing and systems (ICMCS), 10–12 May 2012

Arène C, Lange T, Naehrig M, Ritzenthaler C (2011) Faster computation of the Tate pairing. J Number Theory 131:842–857. https://doi.org/10.1016/j.jnt.2010.05.013

Boneh D, Franklin M (2003) Identity-based encryption from the Weil pairing. SIAM J Comput 32:586–615. https://doi.org/10.1137/S0097539701398521

Busch C, Roth V, Meister R (1998) Perspectives on electronic commerce with mobile agents. In: Paper presented at the proceedings of XI amaldi conference on problems of global security, Moscow, Russia

Chung YF, Chen YT, Chen TL, Chen TS (2011) An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce. Exp Syst Appl 38:9900–9907 https://doi.org/10.1016/j.eswa.2011.02.039

De Caro A, Iovino V (2011) jPBC: Java pairing based cryptography. In: 2011 IEEE symposium on paper presented at the computers and communications (ISCC), June 28 2011–July 1 2011

De Mulder Y, Roelse P, Preneel B (2013) Cryptanalysis of the Xiao—Lai White-Box AES Implementation. In: Paper presented at the selected areas in cryptography, 1 Jan 2013

Dodis Y, Katz J, Xu S, Yung M (2003) Strong key-insulated signature schemes. In: Paper presented at the public key cryptography—PKC 2003

Du TC, Li EY, Wei E (2005) Mobile agents for a brokering service in the electronic marketplace. Decis Support Syst 39:371–383. https://doi.org/10.1016/j.dss.2004.01.003

Esparza O, Munoz JL, Tomas-Buliart J, Soriano M (2011) An infrastructure for detecting and punishing malicious hosts using mobile agent watermarking. Wirel Commun Mob Com 11:1446–1462. https://doi.org/10.1002/Wcm.941

Farashahi RR, Fouque P-A, Shparlinski I, Tibouchi M, Voloch J (2013) Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Math Comput 82:491–512

Freeman DM, Satoh T (2011) Constructing pairing-friendly hyperelliptic curves using Weil restriction. J Number Theory 131:959–983. https://doi.org/10.1016/j.jnt.2010.06.003

Gopal PVSSN, Vasudeva Reddy P, Gowri T (2013) New identity based signature scheme using bilinear pairings over elliptic curves. In: 2013 IEEE 3rd International paper presented at the advance computing conference (IACC), 22–23 Feb 2013

Han S, Chang E, Dillon T (2005) Secure e-transactions using mobile agents with agent broker. In: Proceedings of paper presented at the 2005 international conference on services systems and services management, vol 1–2

Icart T (2009) How to hash into elliptic curves. In: Paper presented at the advances in cryptology-CRYPTO 2009

Jansen WA (2000) Countermeasures for mobile agent security. Comput Commun 23:1667–1676. https://doi.org/10.1016/S0140-3664(00)00253-X

Kawahara Y, Kobayashi T, Takahashi G, Takagi T (2011) Faster maptopoint on supersingular elliptic curves in characteristic 3. IEICE Trans Fundam Electron Commun Comput Sci 94:150–155

Kotzanikolaou P, Burmester M, Chrissikopoulos V (2000) Secure Transactions with Mobile Agents in Hostile Environments. In: Paper presented at the information security and privacy, 1 Jan 2000

Lauter K, Shang N (2013) Generating pairing-friendly parameters for the CM construction of genus 2 curves over prime fields. Des Codes Cryptogr 67:341–355. https://doi.org/10.1007/s10623-012-9611-8

Lee B, Kim H, Kim K (2001) Secure mobile agent using strong non-designated proxy signature. In: Proceedings of paper presented at the information security and privacy

Object Management Group (OMG) (1997) Mobile agent system interoperability facilities specification. http://www.omg.org

Pointcheval D, Stern J (1996) Security proofs for signature schemes. Adv Cryptol Eurocrypt '96 1070:387–398

Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 13:361–396. https://doi.org/10.1007/s001450010003

Sander T, Tschudin C (1998) Protecting mobile agents against malicious hosts. In: Paper presented at the mobile agents and security, 1 Jan 1998

Shamir A (1985) Identity-based cryptosystems and signature schemes. In: Paper presented at the advances in cryptology

Shi Y, Cao L, Wang X (2004a) A security scheme of electronic commerce for mobile agents uses undetachable digital signatures. In: Paper presented at the Proceedings of the 3rd international conference on information security, 2004

Shi Y, Lin J, Zhang C (2011) A white-box encryption algorithm for computing with mobile agents. J Internet Technol 12:981–993

Shi Y, Wang XP, Cao LM, Ren JX (2004b) Secure mobile agents in electronic commerce by using undetachable signatures from pairings. In: Proceedings of 2004 paper presented at the shaping business strategy in a networked world, vol 1–2

Shi Y, Xiong GY (2013) An undetachable threshold digital signature scheme based on conic curves. Appl Math Inform Sci 7:823–828

Shi Y, Zhao Q, Liu Q (2015) Secure mobile agents in ecommerce with forward-secure undetachable digital signatures. ETRI J 37:573–583. https://doi.org/10.4218/etrij.15.0114.0657

Singh R, Dave M (2013) Antecedence graph approach to checkpointing for fault tolerance in mobile agent systems. IEEE Trans Comput 62:247–258. https://doi.org/10.1109/Tc.2011.235

Steinwandt R, Corona AS (2012) Identity-based non-interactive key distribution with forward security. Des Code Cryptogr 64:195–208. https://doi.org/10.1007/s10623-011-9486-0

TaeChan K, Sungwook K, Jung Hee C (2013) On the final exponentiation in tate pairing computations information theory. IEEE Trans Inform Theory 59:4033–4041. https://doi.org/10.1109/TIT.2013.2240763

Tariq MA, Koldehofe B, Rothermel K (2014) Securing broker-less publish/subscribe systems using identity-based encryption. IEEE Trans Parall Distrib 25:518–528. https://doi.org/10.1109/Tpds.2013.256

Trappey AJC, Trappey CV, Lin FTL (2006) Automated silicon intellectual property trade using mobile agent technology. Robot Comput Integr Manuf 22:189–202. https://doi.org/10.1016/j.rcim.2005.03.003

Wang G, Wong TN, Wang XH (2014) A hybrid multi-agent negotiation protocol supporting agent mobility in virtual enterprises. Inform Sci 282:1–14. https://doi.org/10.1016/j.ins.2014.06.021

Wong TN, Fang F (2010) A multi-agent protocol for multilateral negotiations in supply chain management. Int J Prod Res 48:271–299. https://doi.org/10.1080/00207540802425393

Wyseur B (2009) White-box cryptography. PhD Dissertation, Katholieke Universiteit Leuven, B. Preneel (promotor)