Mobile Information Systems 10 (2014) 407–425
DOI 10.3233/MIS-140190
IOS Press

Efficient hierarchical identity-based encryption for Mobile Ad hoc Networks

Kai He[a,*], Min-Rong Chen[b,c], Yijun Mao[d,e], Xi Zhang[f] and Yiju Zhan[g]
[a]*Department of Computer Science, Jinan University, Guangzhou, Guangdong, China*
[b]*College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China*
[c]*School of Computer, South China Normal University, Guangzhou, Guangdong, China*
[d]*School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, Guangdong, China*
[e]*College of Informatics, South China Agricultural University, Guangzhou, Guangdong, China*
[f]*College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, Guangdong, China*
[g]*School of engineering, Sun Yat-Sen University, Guangzhou, Guangdong, China*

Abstract. A Mobile Ad-hoc Network (MANET) is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. Such networks are more vulnerable to security attacks than conventional wired networks, and hence cryptographic schemes are usually used to ensure security for them. It is worth noting that the nodes in MANETs are with low computational power and communicate over relatively bandwidth constrained wireless links, and thus the deployed cryptographic schemes should usually be highly efficient in term of both computational cost and communication overhead. To ensure the data confidentiality for MANETs, in this paper, we present a new hierarchical identity-based encryption (HIBE) scheme, which enjoys the advantages of low computational cost and light communication overhead. We further propose a new hierarchical identity-based key encapsulation mechanism (HIBKEM) based on our HIBE scheme. The proposed HIBKEM scheme is fully secure against adaptive chosen-ciphertext attack, and has a tight security reduction in the standard model.

Keywords: Hierarchical identity-based encryption, key encapsulation mechanism, tight reduction, standard model

1. Introduction

Mobile Ad-hoc Networks (MANETs) consists of a collection of wireless nodes which can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure [36]. Since MANETs require less or no fixed infrastructure support, communications among these nodes can be quickly and adaptively constructed. Such a property ensures that MANETs are especially suitable for communications in critical applications. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks.

However, due to the wireless, resource-constrained, bandwidth-limited, and dynamic nature, MANETs are more vulnerable to security attacks compared with conventional wireless networks [30,42]. Thus

*Corresponding author: Kai He, Department of Computer Science, Jinan University, Guangzhou 510632, Guangdong, China. E-mail: hekai1214@gmail.com.

cryptography is then used to deal with these problems [34]. Cryptography techniques used in MANETs can be classified into two categories, i.e., Symmetric Key based and Asymmetric Key based [41]. In symmetric key based systems, if an attacker compromises the symmetric key of a group of nodes, then all encrypted messages for this group will be exposed. Asymmetric key based schemes can provide more functionalities than symmetric ones, e.g., the key distribution is much easier, compromise of a private key of a node does not reveal messages encrypted for other nodes in the group.

Traditional asymmetric cryptography relies on a Public Key Infrastructure (PKI). The success of PKI depends on the availability and security of a central control point named a Certificate Authority (CA), which issues digital certificates to bind the users and their corresponding public keys. However, in general MANETs, applying PKIs by maintaining a central control point is clearly not always feasible. Another obstacle that applying PKI in MANETs is the heavy overhead of transmission and storage of public key certificates.

In Crypto'84, Shamir [39] introduced a innovative concept named Identity-based cryptography, in which where a user's public key is determined as any publicly known string which represents the user, e.g., email address, domain name, or a physical IP address. Since this identity information is a natural link to a user, there is no need to use digital certificates to bind the users and their corresponding public keys, and hence it can eliminate the requirement of a CA and PKCs. Compared with traditional asymmetric cryptography, identity-based cryptography is more suitable for MANETs. As summarized in [25, 43], identity-based cryptography has the following advantages for MANETs: (i) Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing "free" pairwise keys without any interaction between nodes; (ii) Its resource requirements, regarding process power, storage space, communication bandwidth, are much lower; (iii) The public key of identity-based cryptography is self-proving and can carry much useful information.

Identity-based encryption (IBE) [7,19], an important primitive in identity-based cryptography, can be used to ensure the data confidentiality for MANETs. In identity-based encryption systems, an authority named private key generator (PKG) is in charge of the generation of private keys for the system-wide users. However, if the number of users is huge, then the workload of the PKG would be too heavy, which will cause a bottleneck problem. To reduce the workload of the PKG, hierarchical identity-based encryption (HIBE) was put forth [26,27]. HIBE is a generalization of IBE that mirrors an organizational hierarchy. The PKG only needs to generate private keys for domain-level PKGs, who in turn generate private keys for their users in the lower-level domain. For example, the private key for an entity with identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$ can be generated by his parent identity $\mathsf{ID}_{|k-1} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_{k-1})$. Thus the bottleneck problem of the PKG can be greatly reduced. Hence, HIBE is more suitable for MANETs compared with IBE. In this paper, we shall propose an efficient HIBE scheme to ensure the data confidentiality for MANETs.

1.1. Previous work

Boneh and Franklin [7] proposed the first secure and truly practical IBE, which is provably secure in the random oracle model [13]. However, a proof in the random oracle model can only serve as a heuristic argument and does not imply the security in the real world [17,18]. Therefore, IBE systems provably secure without random oracles attract great interests. Boneh and Boyen [3] initially proposed an IBE scheme which is secure without random oracles under a weaker "selective-ID" model [15]. The same authors later proposed an IBE scheme [4] which is secure in the full model – i.e., *one in which the adversary may choose the target identity adaptively* – without random oracles, albeit less

efficient. Subsequently, Waters [40] proposed an elegant IBE which significantly improves the efficiency of the scheme described in [3]. Waters' construction was modified in [35,37] to allow a controllable tradeoff between the size of the public parameters and the efficiency of the protocol. However, the public parameters in these schemes are still somewhat long, and the security reductions are loose. A loose reduction implies a lower security level or the requirement of larger keys and ciphertext sizes to obtain the same security level.

Somewhat surprisingly, in Eurocrypt'06, Gentry [24] was able to propose the first practical IBE scheme which is secure in the full model without random oracles, yet has short public parameters and a tight security reduction. Interestingly, Gentry's IBE also provides recipient anonymity automatically. However, the provable security is related to a stronger assumption called truncated decisional q-augmented bilinear Diffie-Hellman exponent (q-ABDHE) assumption. Besides, as argued by Gentry himself [24], it is not even obvious what "a tight reduction from decisional q-ABDHE" means, since the assumption is not fixed and it becomes stronger as the number of private key queries increases. What's more, it is still unknown how to extend his IBE to a HIBE system. Recently, Boyen [12] has presented an interesting method to transform exponent inversion IBE into HIBE. Unfortunately, as indicated in [12], since Gentry's IBE scheme fails the exponent inversion litmus test that session keys be of the form v^s for fixed v, Boyen's method cannot be applied to Gentry's IBE. A natural question is whether we can construct another practical IBE system, which is fully secure without random oracles, has short public parameters and a tight security reduction under a fixed assumption (independent of the number of private key queries), and yet can be extended to HIBE systems. In this paper, we shall deal with this problem.

The aforementioned IBE systems secure in the standard model are constructed using bilinear parings. Excitingly, Boneh, Gentry and Hamburg [9] was able to propose a space-efficient IBE scheme in the standard model without using bilinear pairings, albeit the private key size is somewhat large. So far, no HIBE scheme without using bilinear pairings has been proposed.

The first construction of HIBE is due to Gentry and Silverberg [26] where the security is based on the random oracle model. Subsequently, Boneh and Boyen [3] presented a HIBE without random oracles in the selective-ID model. Chatterjee and Sarkar [21] describes a HIBE which is built on the suggestion in [40] by reducing the number of public parameters. In all these constructions, the sizes of ciphertexts and private keys, as well as the decryption cost, grow linearly with the identity depth. Boneh et al. [5] proposed the first HIBE system with constant size ciphertext and without random oracles, whereas the provable security is under the selective-ID model. To achieve the full security, their scheme suffers a security degradation exponential in the hierarchy depth. Chatterjee and Sarkar [23] modified the BBG-HIBE to obtain two variants with constant size ciphertext. The first variant is proved to be secure in a generalization of the selective-ID model. The second one is secure in the full model, whereas the security reduction is loose.

1.2. Our contributions

We present a new HIBE scheme which has several advantages: both the ciphertext size and the decryption cost are independent of the hierarchy depth, and thus it enjoys the advantages of low computational cost and light communication overhead; it is fully secure without random oracles and has a tight security reduction. Therefore our proposed scheme is quite suitable for MANETs. Based on our HIBE system, a new hierarchical identity-based key encapsulation mechanism (HIBKEM) is also presented. The proposed scheme is adaptive chosen-ciphertext secure without using the hierarchical techniques [10,16]. Again, the system is secure in the full model without random oracles and tightly related to the decisional 2-MBDHE assumption. Furthermore, the decapsulation cost is constant, and the ciphertext consists of only two group elements, regardless of the identity depth.

1.3. Organization

The rest of this paper is organized as follows. Section 2 gives an introduction to bilinear pairings, target collision-resistant hash function and some complexity assumptions. The frameworks of HIBE and HIBKEM are also reviewed in this section. We present our HIBE system in Section 3 and prove its security in the full model without random oracles. A comparison between our scheme and other HIBE schemes is also given. In Section 4, we propose a direct chosen-ciphertext secure HIBKEM scheme based on our HIBE scheme. Finally, Section 5 concludes this paper.

2. Preliminaries

2.1. Notations

Throughout this paper, let $\mathbb{Z}_p$ denote the set $\{0, 1, 2, \cdots, p-1\}$, and $\mathbb{Z}_p^*$ denote $\mathbb{Z}_p \backslash \{0\}$. For a finite set S, $x \stackrel{\$}{\leftarrow} \mathcal{S}$ means choosing an element $x \in S$ with a uniform distribution. A function $\nu : \mathbb{N} \rightarrow [0, 1]$ is said to be *negligible* if for all $c \in \mathbb{N}$ there exists a $k_c \in \mathbb{N}$ such that $\nu(k) < k^{-c}$ for all $k > k_c$. Finally, throughout this paper, we often equate a user with his identity.

2.2. Bilinear pairings

Let $\mathbb{G}$ be a cyclic multiplicative group of prime order p, and $\mathbb{G}_T$ be a cyclic multiplicative group of the same order p. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in \mathbb{G}, \forall a, b \in \mathbb{Z}_p^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
- Non-degeneracy: There exist $g_1, g_2 \in \mathbb{G}$ such that $e(g_1, g_2) \neq 1$;
- Computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for $\forall g_1, g_2 \in \mathbb{G}$.

2.3. Target collision resistant hash function

The notion of target collision resistant (TCR) family of hash functions was shown by Cramer and Shoup [20]. In a TCR family, given a randomly chosen hash function H and a random elements x from the definition domain of H, it is infeasible for a polynomial-time adversary $\mathcal{H}$ to find $y \neq x$ such that $H(x) = H(y)$. Informally, we define the advantage of adversary $\mathcal{H}$ in attacking the target collision resistance of H as

$$\mathrm{Adv}_{\mathcal{H},H}^{\mathrm{TCR}} \triangleq \Pr[\mathcal{H} \text{ succeeds}].$$

A TCR family is said to be target collision resistant if the advantage $\mathrm{Adv}_{\mathcal{H},H}^{\mathrm{TCR}}$ is negligible for any polynomial-time adversary $\mathcal{H}$ and any hash function H chosen from this TCR family.

In practice, to build a target collision resistant hash function H, one can use a dedicated cryptographic hash function, like SHA-1 [38]. For that reason and to simplify our presentation, hereafter, we will consider the hash function H to be a fixed function.

2.4. Complexity assumptions

We here recall the q-bilinear Diffie-Hellman exponent (q-BDHE) assumption, which has been used to construct an efficient HIBE scheme in [5]. The q-BDHE assumption is stated as follows: Given a vector of $2q+1$ elements

$$\left(g', g, g^{\alpha}, g^{(\alpha^2)}, \cdots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \cdots, g^{(\alpha^{2q})}\right) \in \mathbb{G}^{2q+1}$$

as input, output $e\left(g, g'\right)^{(\alpha^{q+1})}$. Since the input vector is missing the term $g^{(\alpha^{q+1})}$, the bilinear map does not seem to help compute $e\left(g, g'\right)^{(\alpha^{q+1})}$.

For convenience, hereafter, we use g_i and g'_i to denote $g^{(\alpha^i)}$ and $g'^{(\alpha^i)}$ respectively. Gentry [24] defined an almost identical assumption named q augmented bilinear Diffie-Hellman exponent (q-ABDHE) assumption: Given a vector of $2q+2$ elements

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}\right) \in \mathbb{G}^{2q+2}$$

as input, output $e\left(g_{q+1}, g'\right)$. Introducing the additional term g'_{q+2} still does not appear to help compute $e\left(g_{q+1}, g'\right)$, since the term $g^{(\alpha^{-1})}$ is missed in the input vector.

We here further modify the q-ABDHE assumption by introducing another additional term g_{2q+1}. That is, given a vector of $2q+3$ elements

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}\right) \in \mathbb{G}^{2q+3}$$

as input, output $e\left(g_{q+1}, g'\right)$. Again, introducing the additional term g_{2q+1} still does not appear to help compute $e\left(g_{q+1}, g'\right)$, since the input vector is missing the term $g'^{(\alpha^{-q})}$. We refer to this modified assumption as q modified bilinear Diffie-Hellman exponent (q-MBDHE) assumption.

Note that the q-ABDHE problem is actually more than the requirement for Gentry's IBE. Instead, Gentry [24] introduced a truncated version of the q-ABDHE problem, in which the terms $\left(g_{q+2}, \cdots, g_{2q}\right)$ are omitted from the input vector. Gentry's IBE is based on the decisional version of truncated q-ABDHE. Roughly speaking, the decisional truncated q-ABDHE is, given a random element $Z \in \mathbb{G}_T$ and a vector $\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q\right) \in \mathbb{G}^{q+3}$, to decide whether $Z = e\left(g_{q+1}, g'\right)$.

Our proposed HIBE scheme is based on the decisional q-MBDHE assumption. Formally,

Definition 1. *The **decisional q-MBDHE problem** in groups $(\mathbb{G}, \mathbb{G}_T)$ is, given a vector*

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}\right) \in \mathbb{G}^{2q+3}$$

*for unknown $\alpha \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and the random element $Z \in \mathbb{G}_T$, to decide whether $Z = e\left(g_{q+1}, g'\right)$. For a probabilistic polynomial-time adversary $\mathcal{B}$, we define his **advantage** against the decisional q-MBDHE problem in groups $(\mathbb{G}, \mathbb{G}_T)$ as*

$$Adv^{q\text{-}MBDHE}_{\mathcal{B},(\mathbb{G},\mathbb{G}_T)} \triangleq \Big| Pr\left[\mathcal{B}\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}, e(g_{q+1}, g')\right) = 1\right] - Pr\left[\mathcal{B}\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}, Z\right) = 1\right] \Big|,$$

where the probability is taken over the random bits consumed by $\mathcal{B}$, the random choices of $g, g' \in \mathbb{G}, \alpha \in \mathbb{Z}_p^*$ and $Z \in \mathbb{G}_T$.

Definition 2. *We say that the (t, ϵ) **decisional q-MBDHE assumption** holds in groups $(\mathbb{G}, \mathbb{G}_T)$, if no t-time adversary $\mathcal{B}$ has advantage at least ϵ in solving the decisional q-MBDHE problem in $(\mathbb{G}, \mathbb{G}_T)$.*

2.5. Hierarchical identity-based encryption

Like an IBE system, a HIBE consists of four algorithms: Setup, Extract, Encrypt, Decrypt. In HIBE, however, a vector of dimension k represents an identity at depth k in the hierarchy, and the private key for an identity is generated by his parent. Concretely, a HIBE system Π consists of the following algorithms:

Setup(κ, l)**:** Takes as input a security parameter κ and the maximum hierarchy depth l. It generates the public parameters $param$ and the corresponding master secret key msk.

Extract$(\mathsf{ID}, sk_{\mathsf{ID}_{|k-1}})$**:** Takes as input an identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$ of depth $k \leqslant l$, and the private key $sk_{\mathsf{ID}_{|k-1}}$ of the parent identity $\mathsf{ID}_{|k-1} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_{k-1})$ at depth $k-1$. It outputs the private key sk_{ID} for identity ID.

Encrypt$(m, param, \mathsf{ID})$**:** Takes as input a message m, the public parameters $param$ and an identity ID with a depth less than l. It outputs a ciphertext C.

Decrypt(C, sk_{ID})**:** Takes as input a ciphertext C and the private key sk_{ID} of the recipient ID. It outputs a plaintext m.

Consistency requires that for any message m, any identity ID with a depth less than l, $\mathsf{Decrypt}(C, sk_{\mathsf{ID}}) = m$ always holds, where $C = \mathsf{Encrypt}(m, param, \mathsf{ID})$.

The adaptive chosen-ciphertext security for a HIBE systems Π under a chosen identity attack is defined by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:

Setup: The challenger $\mathcal{C}$ runs algorithm Setup and forwards $param$ to adversary $\mathcal{A}$, keeping the master secret key msk itself.

Phase 1: Adversary $\mathcal{A}$ adaptively issues queries $q_1, \cdots, q_m$ where q_i is one of the following:

- Private key query $\langle \mathsf{ID} \rangle$: $\mathcal{C}$ runs algorithm Extract to generate the corresponding private key sk_{ID}, which is returned to $\mathcal{A}$.
- Decryption query $\langle \mathsf{ID}, C \rangle$: $\mathcal{C}$ runs algorithm Extract to generate the private key sk_{ID}. It then runs algorithm Decrypt to decrypt the ciphertext C using the private key sk_{ID}. The resulting plaintext m is returned to $\mathcal{A}$.

Challenge: Once $\mathcal{A}$ decides that Phase 1 is over, it outputs a target identity ID^* and two equal-length messages m_0, m_1. The only restriction is that, $\mathcal{A}$ did not previously issue a private key query for ID^* or a prefix of ID^*. $\mathcal{C}$ flips a random coin $b \in \{0, 1\}$ and sets the challenge ciphertext to $C^* = \mathsf{Encrypt}(m_b, param, \mathsf{ID}^*)$, which is sent to $\mathcal{A}$.

Phase 2: This is identical to Phase 1, except that $\mathcal{A}$ can not issue a private key query for ID^* or a prefix of ID^*, and $\mathcal{A}$ can not issue a decryption query for $\langle \mathsf{ID}^*, C^* \rangle$.

Guess: Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins if $b' = b$.

We refer to such an adversary $\mathcal{A}$ as an IND-ID-CCA2 adversary. We define $\mathcal{A}$'s advantage in attacking the scheme Π as $\mathrm{Adv}^{\text{IND-ID-CCA2}}_{\mathcal{A},\Pi} \triangleq \left|\Pr[b = b'] - \frac{1}{2}\right|$, where the probability is taken over the random coins consumed by the challenger and the adversary.

Boneh et al. [5] defined a weaker security notion for HIBE systems, i.e., adaptive chosen-ciphertext security under a selective-ID attack (IND-sID-CCA2). The IND-sID-CCA2 game is exactly the same as IND-ID-CCA2 except that the adversary $\mathcal{A}$ must commit to the target identity ID^* before the Setup phase.

Definition 3. *We say that a HIBE system Π is (t, q_e, q_d, ϵ)-IND-ID-CCA2 (resp. IND-sID-CCA2) secure, if for any t-time IND-ID-CCA2 (resp. IND-sID-CCA2) adversary $\mathcal{A}$ who makes at most q_e private key queries and at most q_d decryption queries, we have that $Adv^{\text{IND-ID-CCA2}}_{\mathcal{A},\Pi} < \epsilon$ (resp. $Adv^{\text{IND-sID-CCA2}}_{\mathcal{A},\Pi} < \epsilon$).*

The chosen-plaintext security for a HIBE system Π can be defined as the preceding game, except that adversary $\mathcal{A}$ is disallowed to issue any decryption query. This security notion is termed as IND-ID-CPA (or IND-sID-CPA in the case of a selective-ID adversary).

Definition 4. *We say that a HIBE system* Π *is* (t, q_e, ϵ)*-IND-ID-CPA (resp. IND-sID-CPA) secure if* Π *is* $(t, q_e, 0, \epsilon)$*-IND-ID-CCA2 (resp. IND-sID-CCA2) secure.*

2.6. Hierarchical identity-based key encapsulation

A hierarchical identity-based key encapsulation mechanism (HIBKEM) consists of four algorithms, i.e., Setup, Extract, Encap and Decap, where algorithms Setup and Extract are the same as in HIBE systems, and algorithms Encap and Decap are depicted as below:

Encap$(param, \mathsf{ID})$**:** Takes as input the public parameters $param$ and an identity ID with a depth less than l. It outputs a random session key K and a corresponding ciphertext C with respect to identity ID.

Decap(C, sk_{ID})**:** Takes as input a ciphertext C, the private key sk_{ID} of the recipient ID. It outputs either $\perp$ or the corresponding session key K.

For consistency, we require that for any $\kappa, l \in \mathbb{N}$, any identity ID with a depth less than l, $\mathsf{Decap}(C, sk_{\mathsf{ID}}) = K$ always holds, where $(C, K) = \mathsf{Encap}(param, \mathsf{ID})$.

The IND-ID-CCA2 security for a HIBKEM system Π' is defined by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:

Setup: The same as in the IND-ID-CCA2 game for HIBE systems.

Phase 1: $\mathcal{A}$ adaptively issues $q_1, \cdots, q_m$ where q_i is one of the following:

- Private key query $\langle \mathsf{ID} \rangle$: The same as in the IND-ID-CCA2 game for HIBE systems.
- Decapsulation query $\langle \mathsf{ID}, C \rangle$: $\mathcal{C}$ responds by running algorithm Extract to generate the private key sk_{ID}. It then runs algorithm Decap to decrypt the ciphertext C using the private key sk_{ID}, and sends the resulting session key K to $\mathcal{A}$.

Challenge: Once $\mathcal{A}$ decides that Phase 1 is over, it outputs a target identity ID^*. The only restriction is that, $\mathcal{A}$ did not previously issue a private key query for ID^* or a prefix of ID^*. $\mathcal{C}$ first runs algorithm $\mathsf{Encap}(param, \mathsf{ID}^*)$ to generate a random session key K_1^*, and then picks a random element K_0^* from the session key space. Finally, $\mathcal{C}$ flips a random coin $b \in \{0, 1\}$, and gives (C^*, K_b^*) to $\mathcal{A}$.

Phase 2: This is identical to Phase 1, except that $\mathcal{A}$ can not issue a private key query for ID^* or a prefix of ID^*, and $\mathcal{A}$ can not issue a decapsulation query for $\langle \mathsf{ID}^*, C^* \rangle$.

Guess: Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins if $b = b'$.

We define the advantage of $\mathcal{A}$ in the above game as $\mathrm{Adv}^{\text{IND-ID-CCA2}}_{\mathcal{A},\Pi'} \triangleq \left|\Pr[b = b'] - \frac{1}{2}\right|$, where the probability is taken over the random coins consumed by the challenger and the adversary.

Definition 5. *We say that a HIBKEM system* Π' *is* (t, q_e, q_d, ϵ)*-IND-ID-CCA2 secure, if for any* t*-time adversary* $\mathcal{A}$ *who makes at most* q_e *private key queries and at most* q_d *decapsulation queries, we have that* $Adv^{IND\text{-}ID\text{-}CCA2}_{\mathcal{A},\Pi'} < \epsilon$.

3. Proposed HIBE scheme: Chosen-plaintext security

In this section, we present a new constant size HIBE system, and then prove its IND-ID-CPA security in the standard model. A comparison between our HIBE system and other HIBE systems is also given.

3.1. Construction

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups with prime order p of size κ, and let e be a bilinear map such that $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The proposed HIBE scheme consists of the following algorithms:

Setup(κ, l)**:** To generate system parameters for a HIBE of maximum hierarchy depth l, the PKG first randomly picks $u_1, g \overset{\$}{\leftarrow} \mathbb{G}$, $\alpha \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and sets $g_1 = g^\alpha$. Next, for each $i \in \{2, \cdots, l\}$ it picks w_i and an n-length vector $\vec{U}_i = (u_{i,1}, \cdots, u_{i,n})$ with $u_{i,j} \overset{\$}{\leftarrow} \mathbb{G}$, $j = 1, \cdots, n$. The public parameter

$$param = (g, g_1, u_1, w_2, \cdots, w_l, \vec{U}_2, \cdots, \vec{U}_l), \qquad msk = \alpha.$$

Extract(msk, ID)**:** To generate a private key sk_{ID_1} for a first-level identity ID_1, the PKG picks $r_1 \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and define the private key as

$$\begin{aligned} sk_{\mathsf{ID}_1} = \Big(& (r_1, (g^{r_1} u_1)^{\frac{1}{\alpha - \mathsf{ID}_1}}), w_2^{\frac{1}{\alpha - \mathsf{ID}_1}}, (r_{2,1}, (g^{r_{2,1}} u_{2,1})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{2,n}, (g^{r_{2,n}} u_{2,n})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \\ & w_3^{\frac{1}{\alpha - \mathsf{ID}_1}}, (r_{3,1}, (g^{r_{3,1}} u_{3,1})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{3,n}, (g^{r_{3,n}} u_{3,n})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \\ & \vdots \\ & w_l^{\frac{1}{\alpha - \mathsf{ID}_1}}, (r_{l,1}, (g^{r_{l,1}} u_{l,1})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{l,n}, (g^{r_{l,n}} u_{l,n})^{\frac{1}{\alpha - \mathsf{ID}_1}}) \Big) \end{aligned} \tag{1}$$

Now, user ID_1 can generate the private key for his children $\mathsf{ID} = (\mathsf{ID}_1, \mathsf{ID}_2)$ as

$$\begin{aligned} sk_{\mathsf{ID}} = \Big(& \Big(r_1 + F(2, \mathsf{ID}_2) \sum_{j_2 \in \mathcal{V}_{\mathsf{ID}_2}} r_{2,j_2}, \Big(g^{r_1 + F(2,\mathsf{ID}_2) \sum_{j_2 \in \mathcal{V}_{\mathsf{ID}_2}} r_{2,j_2}} u_1 \big(w_2 \prod_{j_2 \in \mathcal{V}_{\mathsf{ID}_2}} u_{2,j_2} \big)^{F(2,\mathsf{ID}_2)} \Big)^{\frac{1}{\alpha - \mathsf{ID}_1}} \Big), \\ & w_3^{\frac{1}{\alpha - \mathsf{ID}_1}}, (r_{3,1}, \big(u_{3,1} g^{r_{3,1}} \big)^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{3,n}, \big(u_{3,n} g^{r_{3,n}} \big)^{\frac{1}{\alpha - \mathsf{ID}_1}}), \\ & \vdots \\ & w_l^{\frac{1}{\alpha - \mathsf{ID}_1}}, (r_{l,1}, \big(u_{l,1} g^{r_{l,1}} \big)^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{l,n}, \big(u_{l,n} g^{r_{l,n}} \big)^{\frac{1}{\alpha - \mathsf{ID}_1}}) \Big) \end{aligned}$$

Similarly, we can see that the private key for a k-level identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$ is

$$\begin{aligned} sk_{\mathsf{ID}} = \Big(& \Big(r_1 + \sum_{i=2}^{k} \big(F(i, \mathsf{ID}_i) \sum_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} r_{i,j_i} \big), \\ & \Big(g^{r_1 + \sum_{i=2}^{k} \Big(F(i,\mathsf{ID}_i) \sum_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} r_{i,j_i} \Big)} u_1 \prod_{i=2}^{k} \big(w_i \prod_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} u_{i,j_i} \big)^{F(i,\mathsf{ID}_i)} \Big)^{\frac{1}{\alpha - \mathsf{ID}_1}} \Big), \\ & (r_{k+1,1}, (u_{k+1,1} g^{r_{k+1,1}})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{k+1,n}, (u_{k+1,n} g^{r_{k+1,n}})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \\ & \vdots \\ & (r_{l,1}, (u_{l,1} g^{r_{l,1}})^{\frac{1}{\alpha - \mathsf{ID}_1}}), \cdots, (r_{l,n}, (u_{l,n} g^{r_{l,n}})^{\frac{1}{\alpha - \mathsf{ID}_1}}) \Big) \end{aligned}$$

Encrypt$(m, param, \mathsf{ID})$**:** To encrypt a message $m \in \mathbb{G}_T$ under an identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$, pick $s \in \mathbb{Z}_p^*$ and output

$$C = \left(\left(g_1 g^{-\mathsf{ID}_1}\right)^s, e(g,g)^s, m \cdot e\left(g, u_1 \prod_{i=2}^{k} \left(w_i \prod_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} u_{i,j_i} \right)^{F(i,\mathsf{ID}_i)} \right) \right)^s. \tag{2}$$

Decrypt(C, sk_{ID})**:** Given a ciphertext $C = (C_1, C_2, C_3)$ for identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$, one can use the private key sk_{ID} to decrypt this ciphertext as below:

$$m = \frac{C_3 \cdot C_2^{r_1 + \sum_{i=2}^{k} \left(F(i,\mathsf{ID}_i) \sum_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} r_{i,j_i} \right)}}{e\left(C_1, \left(g^{r_1 + \sum_{i=2}^{k} \left(F(i,\mathsf{ID}_i) \sum_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} r_{i,j_i} \right)} u_1 \prod_{i=2}^{k} \left(w_i \prod_{j_i \in \mathcal{V}_{\mathsf{ID}_i}} u_{i,j_i} \right)^{F(i,\mathsf{ID}_i)} \right)^{\frac{1}{\alpha - \mathsf{ID}_1}} \right)}.$$

3.2. Security analysis

Theorem 1. *Assume that the (t', ϵ') decisional 2-MBDHE assumption holds in $(\mathbb{G}, \mathbb{G}_T)$. Then the proposed HIBE scheme is (t, q_e, ϵ)-IND-ID-CPA secure with*

$$t' = t + \mathcal{O}(q_e \cdot l \cdot t_{exp}), \quad \epsilon' = \epsilon,$$

where q_e denotes the number of private key queries, l is the maximal hierarchy depth, and t_{exp} denotes the running time of an exponentiation in $\mathbb{G}$.

Proof. Suppose there exists a (t, q_e, ϵ) adversary $\mathcal{A}$ against the IND-ID-CPA security of our HIBE scheme. Using $\mathcal{A}$, we can construct an algorithm $\mathcal{B}$ that solves the (t', ϵ') decisional 2-MBDHE assumption in $(\mathbb{G}, \mathbb{G}_T)$. Taking as input a random decisional 2-MBDHE challenge $(g', g'_4, g, g_1, g_2, g_4, g_5, Z)$, where Z is either $e(g_3, g')$ or a random element in $\mathbb{G}_T$, algorithm $\mathcal{B}$'s goal is to output 1 when $Z = e(g_3, g')$ and 0 otherwise. Recall that we use g'_i and g_i to denote $g'^{(\alpha^i)}$ and $g^{(\alpha^i)}$ respectively. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in the IND-ID-CPA game as below:

Setup: To generate the public parameters for $\mathcal{A}$, using a trick similar to that in [24], algorithm $\mathcal{B}$ works as follows:

1. Pick $\delta \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. Without loss of generality, we assume that $\delta \neq \alpha$, since if $\delta = \alpha$, $\mathcal{B}$ can use δ to solve the decisional 2-MBDHE challenge immediately. A random polynomial $F_1(x) \in \mathbb{Z}_p[x]$ of degree 2 is also generated.
2. Set $w = g, w_1 = g_1 g^{-\delta} = w^{\alpha - \delta}, w_2 = g^{F_1(\alpha)} g^{-F_1(\delta)}$ and $Y = e(w, w_2)$. Note that w_2 can be computed from (g, g_1, g_2) and δ. Due to the randomness of δ and $F_1(x)$, w_1 and w_2 are independent of each other and randomly distributed in $\mathbb{G}$. Observe that if let $\beta = \alpha - \delta$, then w_1 is well-formed as required.
3. Pick $v', v_1, \cdots, v_l \overset{\$}{\leftarrow} \mathbb{Z}_p^*$, set $h' = w_1^{v'}$ and $h_i = w_1^{v_i}$ for $i = 1, \cdots, l$. The public parameter $param = (w_1, Y, h', h_1, \cdots, h_l)$ is sent to $\mathcal{A}$.

Observe that the distribution of these public parameters is identical to that in the real construction. Let $F_2(x)$ denote the 1-degree polynomial $\frac{F_1(x)-F_1(\delta)}{x-\delta}$, then $\mathcal{B}$ can compute the master secret key as $msk = g^{F_2(\alpha)}$, which can be computed from (g, g_1). Note that this is a valid master secret key as required, since $g^{F_2(\alpha)} = g^{\frac{F_1(\alpha)-F_1(\delta)}{\alpha-\delta}} = w_2^{\frac{1}{\alpha-\delta}} = w_2^{\frac{1}{\beta}}$.

Phase 1: In this phase, $\mathcal{A}$ issues a series of private key queries. Upon receiving a private key query on identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$, $\mathcal{B}$ can certainly construct a valid private key for adversary $\mathcal{A}$ as Eq. (1), since $\mathcal{B}$ knows the master secret key msk.

Challenge: When $\mathcal{A}$ decides that Phase 1 is over, it outputs an identity $\mathsf{ID}^* = (\mathsf{ID}_1^*, \cdots, \mathsf{ID}_k^*) \in \left(\mathbb{Z}_p^*\right)^k$ and two equal-length messages $m_0, m_1 \in \mathbb{G}_T$. Let $F_3(x) = x^4$ and let $F_4(x) = \frac{F_3(x)-F_3(\delta)}{x-\delta}$, which is a polynomial of degree 3. Let $F_5(x) = (F_1(x) - F_1(\delta)) \cdot F_4(x)$, and express $F_5(x)$ as $F_5(x) = \sum_{i=0}^{5} F_{5,i}x^i$, where $F_{5,i}$ is the coefficient of x^i in $F_5(x)$. Algorithm $\mathcal{B}$ picks $b \overset{\$}{\leftarrow} \{0,1\}$ and computes

$$C_1^* = g'^{F_3(\alpha)-F_3(\delta)}, \quad C_2^* = m_b \cdot Z^{F_{5,3}} \cdot e\left(g', \prod_{\substack{i=0 \\ i\neq 3}}^{5} g_i^{F_{5,i}}\right), \quad C_3^* = C_1^{*v'+\sum_{i=1}^{k} v_i \mathsf{ID}_i^*}.$$

The challenge ciphertext $C^* = (C_1^*, C_2^*, C_3^*)$ is returned to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ issues a series of private key queries, and $\mathcal{B}$ responds as in Phase 1.

Guess: Finally, adversary $\mathcal{A}$ returns a guess $b' \in \{0,1\}$ to $\mathcal{B}$. If $b = b'$, then $\mathcal{B}$ outputs 1 indicating $Z = e(g_3, g')$. Otherwise, it outputs 0 indicating Z is a random element in $\mathbb{G}_T$.

Analysis: From the description of the simulation, we can see that the public parameters are well-formed and have an indistinguishable distribution as in the real environment. The responses to $\mathcal{A}$'s private key queries are also perfect. Moreover, if $Z = e\left(g_3, g'\right)$, then C^* is a valid ciphertext for (ID^*, m_b). To see this, let $s = \left(\log_g g'\right) \cdot F_4(\alpha)$, then

$$\begin{aligned}
C_1^* &= g'^{F_3(\alpha)-F_3(\delta)} = g^{\left(\log_g g'\right)\cdot(F_3(\alpha)-F_3(\delta))} = g^{\left(\log_g g'\right)\cdot F_4(\alpha)\cdot(\alpha-\delta)} = g^{s\cdot(\alpha-\delta)} = w_1^s, \\
C_2^* &= m_b \cdot Z^{F_{5,3}} \cdot e\left(g', \prod_{\substack{i=0 \\ i\neq 3}}^{5} g_i^{F_{5,i}}\right) = m_b \cdot e\left(g', g_3\right)^{F_{5,3}} \cdot e\left(g', \prod_{\substack{i=0 \\ i\neq 3}}^{5} g_i^{F_{5,i}}\right) \\
&= m_b \cdot e\left(g', \prod_{i=0}^{5} g_i^{F_{5,i}}\right) = m_b \cdot e\left(g', g\right)^{\sum_{i=0}^{5} F_{5,i}\alpha^i} = m_b \cdot e\left(g, g\right)^{\left(\log_g g'\right)\cdot F_5(\alpha)} \\
&= m_b \cdot e\left(g, g\right)^{\left(\log_g g'\right)\cdot F_4(\alpha)\cdot(F_1(\alpha)-F_1(\delta))} = m_b \cdot e\left(g, g^{F_1(\alpha)-F_1(\delta)}\right)^s = m_b \cdot e\left(w, w_2\right)^s \\
&= m_b \cdot Y^s, \\
C_3^* &= C_1^{*v'+\sum_{i=1}^{k} v_i \mathsf{ID}_i^*} = w_1^{s\cdot\left(v'+\sum_{i=1}^{k} v_i \mathsf{ID}_i^*\right)} = \left(w_1^{v'} \cdot \prod_{i=1}^{k} w_1^{v_i \mathsf{ID}_i^*}\right)^s = \left(h' \prod_{i=1}^{k} h_i^{\mathsf{ID}_i^*}\right)^s.
\end{aligned}$$

So, when $Z = e\left(g_3, g'\right)$, the simulation provided for $\mathcal{A}$ is indistinguishable from the real environment. Hence we see that

$$\Pr\left[\mathcal{B}\left(g', g_4', g, g_1, g_2, g_4, g_5, e(g_3, g')\right) = 1\right] = \frac{1}{2} + \epsilon.$$

Table 1
Comparison of the proposed HIBE scheme with other HIBE schemes

Protocol	Without RO?	Full or selective-ID	Underlying assumption	Tight reduction	Size of Pub. Para.	Size of ciphertext	Pairings Enc.	Pairings Dec.
BB04a[3]	$\surd$	Selective-ID	Dec. BDH	$\surd$	$\mathcal{O}(l)$	$\mathcal{O}(k)$	None	k+1
BB04b[4]	$\surd$	Full	Dec. BDH	$\times$	$\mathcal{O}(n \times l)$	$\mathcal{O}(n \times k)$	None	k+1
Waters05[40]	$\surd$	Full	Dec. BDH	$\times$	$\mathcal{O}(n \times l)$	$\mathcal{O}(k)$	None	k+1
CS06a[21]	$\surd$	Full	Dec. BDH	$\times$	$\mathcal{O}(n + l)$	$\mathcal{O}(k)$	None	k+1
BBG05[5]	$\surd$	Selective-ID	Dec. l-BDHE	$\surd$	$\mathcal{O}(l)$	$\mathcal{O}(1)$	None	2
CS06b[23]	$\surd$	g-Selective-ID	Dec. l-wBDHI*	$\surd$	$\mathcal{O}(n \times l)$	$\mathcal{O}(1)$	None	2
Our Scheme	$\surd$	Full	Dec. 2-MBDHE	$\surd$	$\mathcal{O}(l)$	$\mathcal{O}(1)$	None	2

Notes: l denotes the maximal hierarchy depth, n is the number of bit representing an identity, k represents the depth of an identity.

On the other hand, when Z is uniform and independent in $\mathbb{G}_T$, the challenge ciphertext C^* is independent of b in the adversary's view. Thus we have

$$\Pr\left[\mathcal{B}\left(g', g_4', g, g_1, g_2, g_4, g_5, Z\right) = 1\right] = \frac{1}{2}.$$

Therefore, algorithm $\mathcal{B}$ has an advantage $\epsilon' = \epsilon$ in solving the decisional 2-MBDHE challenge.

In the simulation, the time complexity of $\mathcal{B}$ is dominated by the exponentiations in the private key queries. Since there are $\mathcal{O}(l)$ exponentiations in each query, we know that $\mathcal{B}$'s time complexity is $t' = t + \mathcal{O}(q_e \cdot l \cdot t_{exp})$. This concludes the proof of this theorem. □

3.3. Comparison

In Table 1, the proposed HIBE scheme is compared with other HIBE systems without random oracles. To conduct a fair comparison, we use the chosen-plaintext secure version for all the systems, since there exist generic transformations [10,16] from CPA-secure HIBE to CCA2-secure systems.

HIBE systems secure in the full model without random oracles include BB04b [4], Waters05 [40] and CS06a [21]. However, these schemes suffer from loose security reductions. Furthermore, both the ciphertext size and the decryption cost grow linearly with the identity depth.

HIBE systems with constant size ciphertext include BBG05 [5] and CS06b [23]. The security reductions of these schemes are tight, whereas they are only secure in the selective-ID model. To achieve the full security, it takes a security degradation of $\approx 2^{nh}$. Besides, the underlying assumptions, on which the two schemes are based, become stronger as the the maximal hierarchy depth increases.

As to our scheme, it is secure in the full model without random oracles, the sizes of the ciphertexts as well as the cost for encryption and decryption are constant, and the security reduction is tight, albeit to the non-standard 2-MBDHE assumption. Unlike those assumptions used in [5,23,24], our underlying assumption is related to neither the maximal hierarchy depth nor the number of private key queries. As to Gentry's IBE underlying assumption (decisional truncated q-ABDHE), when the number of private key queries is up to 2^{30}, its complexity lower bound is nearly 2.1×10^8 times greater than ours in the generic bilinear group. However, we stress that, these generic-group results do not imply the results in the real world, since the fastest algorithms for solving these assumptions are likely non-generic.

4. Direct chosen-ciphertext secure HIBKEM scheme

In many applications where one needs to encrypt arbitrary long messages, it is desirable to provide hybrid encryption. A hybrid encryption system consists of two basic operations: one operation uses a

key encapsulation mechanism (KEM) to derive a session key; the other uses the session key in a data encapsulation mechanism (DEM) to encrypt the actual message. There exist a number of interesting results in hybrid encryptions, e.g. [2,20,28]. So far, KEM has also been extended to identity-based scenarios [8,33], and several IBKEM/HIBKEM systems have been proposed. In this section, we consider the construction of a new chosen-ciphertext secure HIBKEM system based on our HIBE scheme.

Recent results from Canetti, Halevi and Katz [16], further improved by Boneh and Katz [10], showed generic transformations from any CPA-secure IBE to a CCA2-secure public key encryption. These generic transformations can also be used to convert a $(l+1)$-level CPA-secure HIBKEM into a l-level CCA2-secure HIBKEM. However, as pointed out in [29], these transformations involve some symmetric overhead to the ciphertext in form of a one-time signature or a MAC with their respective keys. Interestingly, Boneh, Mei and Waters [11] presented a non-generic technique to built direct CCA2-secure public key encryptions from some IBE systems. BMW technique can also be applied to our HIBE to construct an IND-ID-CCA2 secure HIBKEM system. However, the resulting system introduces a ciphertext overhead of one group element, which can be viewed as a checksum of the ciphertext. Recently, based on Waters' IBE system, Kiltz has proposed a direct CCA2-secure IBKEM with short ciphertexts. Based on our HIBE system, we here construct a new HIBKEM system through introducing Kiltz's technique. The proposed HIBKEM system is IND-ID-CCA2 secure in the full model without random oracles, and its ciphertext consists of only two group elements, regardless of the hierarchy depth.

4.1. Construction

As before, let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups with prime order p of size κ, and let e be a bilinear map such that $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Besides, we also use a target collision-resistant hash function H such that $H : \mathbb{G} \to \mathbb{Z}_p^*$. Based on our HIBE system, the HIBKEM scheme is described as follows.

Setup(κ, l)**:** The same as in the proposed HIBE system with the exception that a random group element, $u \xleftarrow{\$} \mathbb{G}$, is included in the public parameters $param$.

Extract$(\mathbf{ID}, sk_{\mathbf{ID}_{|k-1}})$**:** To generate private key sk_{ID} for identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k) \in \left(\mathbb{Z}_p^*\right)^k$ of depth $k \leqslant l$, the PKG picks $r \xleftarrow{\$} \mathbb{Z}_p^*$ and outputs

$$sk_{\mathsf{ID}} = \left(w_2^{\frac{1}{\beta}} \cdot \left(h' \prod_{i=1}^{k} h_i^{\mathsf{ID}_i}\right)^r, w_1^r, u^r, h_{k+1}^r, \cdots, h_l^r\right) \in \mathbb{G}^{3+l-k}. \tag{3}$$

Note that the private key for identity ID can also be generated by its parent $\mathsf{ID}_{|k-1} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_{k-1})$ as required.

Encap$(param, \mathbf{ID})$**:** To encapsulate a random session key under an identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$, pick $s \in \mathbb{Z}_p^*$ and output

$$C = (C_1, C_2) = \left(w_1^s, \left(u^t \cdot h' \prod_{i=1}^{k} h_i^{\mathsf{ID}_i}\right)^s\right), \tag{4}$$

where $t = H(C_1)$. The session key K is calculated by the sender as $K = Y^s \in \mathbb{G}_T$.

Decap$(C, sk_{\mathbf{ID}})$**:** Given a ciphertext $C = (C_1, C_2)$ for identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$, the algorithm first computes $t = H(C_1)$, and then checks whether $(w_1, C_1, u^t \cdot h' \prod_{i=1}^{k} h_i^{\mathsf{ID}_i}, C_2)$ is a Diffie-Hellman tuple.[1] If not, the ciphertext is invalid and this algorithm outputs a random element in

[1] A tuple $(g, g^a, g^b, g^c) \in \mathbb{G}^4$ is said to be a Diffie-Hellman tuple if $ab = c \mod p$.

$\mathbb{G}_T$. Otherwise, using the private key $sk_{\mathsf{ID}} = (a_0, a_1, a_2, b_{k+1}, \cdots, b_l)$, it outputs the session key as

$$K = \frac{e\left(C_1, a_0 \cdot a_2^t\right)}{e\left(C_2, a_1\right)}. \tag{5}$$

Consistency: Indeed, a correctly generated ciphertext for identity $\mathsf{ID} = (\mathsf{ID}_1, \cdots, \mathsf{ID}_k)$ has the correct form as Eq. (4), and hence $(w_1, C_1, u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}, C_2)$ is a Diffie-Hellman tuple. In this case, the session key computed from Eq. (5) is indeed the original session key, since

$$K = \frac{e\left(C_1, a_0 \cdot a_2^t\right)}{e\left(C_2, a_1\right)} = \frac{e\left(w_1^s, w_2^{\frac{1}{\beta}} \cdot \left(h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)^r \cdot (u^r)^t\right)}{e\left(\left(u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)^s, w_1^r\right)}$$

$$= \frac{e\left(w_1^s, w_2^{\frac{1}{\beta}}\right) \cdot e\left(w_1^s, \left(u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)^r\right)}{e\left(\left(u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)^r, w_1^s\right)} = Y^s.$$

More efficient decapsulation: In algorithm Decap, to ensure that $\left(w_1, C_1, u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}, C_2\right)$ is a Diffie-Hellman tuple, one can check whether $e\left(w_1, C_2\right) = e\left(C_1, u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)$ holds. In this case, algorithm Decap needs totally four bilinear parings. Inspired by the idea in [14] (this technique was also used in [29,31]), we can avoid the explicit validity check to get a more efficient decapsulation algorithm.[2] More precisely, we choose a random value $\gamma \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and compute the session key as

$$K = \frac{e\left(C_1, a_0 \cdot a_2^t \cdot \left(u^t \cdot h' \prod_{i=1}^k h_i^{\mathsf{ID}_i}\right)^\gamma\right)}{e\left(C_2, a_1 w_1^\gamma\right)}. \tag{6}$$

Note that this alternative decapsulation algorithm saves one pairing (for the cost of two exponentiations). Similarly to the arguments in [29,31], it can be verified that this alternative algorithm is equivalent to the original decapsulation algorithm.

4.2. Security and comparisons

The validity test of ciphertexts ensures that each decapsulation query is well-formed and will be properly decapsulated. Hence it can prevent an adversary from obtaining any useful information by issuing decapsulation queries on malformed ciphertexts. It is this crucial point that makes our system resist the adaptive chosen-ciphertext attack.

Theorem 2. *Assume H is a TCR hash function. Under the decisional 2-MBDHE assumption in $(\mathbb{G}, \mathbb{G}_T)$, the proposed HIBKEM scheme Π' is IND-ID-CCA2 secure. In particular, we have*

$$Adv_{\mathcal{A},\Pi'}^{\text{IND-ID-CCA2}} \leqslant Adv_{\mathcal{B},(\mathbb{G},\mathbb{G}_T)}^{\text{2-MBDHE}} + Adv_{\mathcal{H},H}^{\text{TCR}}, \tag{7}$$

for any adversary $\mathcal{A}$ against the proposed HIBKEM scheme Π' with running time $\mathsf{Time}_{\mathcal{A}} = \mathsf{Time}_{\mathcal{B}} - \mathcal{O}(l \cdot (q_e + q_d) t_{exp} + q_d \cdot t_{par})$, where q_d denotes the number of decapsulation queries, t_{par} denotes the running time of a pairing in $\mathbb{G}$, and t_{exp}, l and q_e are defined the same as in Theorem 1.

[2] In fact, without using the explicit validity check, the decapsulation algorithm can still learn whether a ciphertext is valid by adopting some tricks in [14].

Before continuing, we review a simple but useful lemma in [20].

Lemma 1. *Let U_1, U_2 and F be the events defined on some probability space. Suppose that the event $U_1 \wedge \neg F$ occurs if and only if $U_2 \wedge \neg F$ occurs. Then $\big|Pr[U_1] - Pr[U_2]\big| \leqslant Pr[F]$.*

Proof. The proof of Theorem 2 is given as a sequence of games. In each game, a bit $b \in \{0,1\}$ is randomly chosen, and the adversary outputs a guess $b' \in \{0,1\}$. By X_i, we denote the event that $b = b'$ in the i-th game.

Game$_0$. This is the original attack game for defining the IND-ID-CCA2 security for HIBKEM systems. We assume that adversary $\mathcal{A}$'s running time is $\mathsf{Time}_{\mathcal{A}}$, and it makes q_e private key queries and q_d decapsulation queries. Clearly, we have

$$\mathrm{Adv}^{\text{IND-ID-CCA2}}_{\mathcal{A},\Pi'} = \big|\Pr[X_0] - \frac{1}{2}\big|. \tag{8}$$

The ciphertext component C_1^* provided for adversary $\mathcal{A}$ during the Challenge phase does not depend on $\mathcal{A}$'s input. We will assume that this is randomly chosen during the Setup phase.

Game$_1$. (Eliminate hash collisions) This game is the same as **Game**$_0$, except for the following modification in the decapsulation oracle: if adversary $\mathcal{A}$ ever submits a ciphertext $C = (C_1, C_2)$ to the decapsulation oracle such that $C_1 \neq C_1^*$ but $H(C_1) = H(C_1^*)$, then the simulation immediately aborts (denote this event by $\mathsf{HashAbort}$). Then we see that **Game**$_0$ and **Game**$_1$ are identical until event $\mathsf{HashAbort}$ happens. Therefore, by Lemma 1 we have

$$\big|\Pr[X_1] - \Pr[X_0]\big| \leqslant \Pr[\mathsf{HashAbort}]. \tag{9}$$

Furthermore,

$$\Pr[\mathsf{HashAbort}] \leqslant \mathrm{Adv}^{\text{TCR}}_{\mathcal{H},\mathrm{H}}. \tag{10}$$

Game$_2$. (Change of the public key) We now modify **Game**$_1$ to obtain a new game **Game**$_2$. These two games are identical, except for a small modification to the generation of the public parameters. The simulator picks $g, g' \overset{\$}{\leftarrow} \mathbb{G}, \alpha \overset{\$}{\leftarrow} \mathbb{Z}_p^*$, and computes $g_4' = g'^{(\alpha^4)}$, $g_i = g^{(\alpha^i)}$ for $i = 1, 2, 4, 5$. Next, it generates the public parameters for $\mathcal{A}$ as below:

1. Pick $\delta \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ (if $\delta = \alpha$, choose δ again). A random polynomial $F_1(x) \in \mathbb{Z}_p[x]$ of degree 2 is also generated.
2. Set $w = g, w_1 = g_1 g^{-\delta} = w^{\alpha-\delta}, w_2 = g^{F_1(\alpha)} g^{-F_1(\delta)}$ and $Y = e(w, w_2)$.
3. Pick $\mu, v', v_1, \cdots, v_l \overset{\$}{\leftarrow} \mathbb{Z}_p^*$, set $u = w_1^{\mu}, h' = w_1^{v'}$ and $h_i = w_1^{v_i}$ for $i = 1, \cdots, l$. The public parameters $param = (u, w_1, Y, h', h_1, \cdots, h_l)$ are given to $\mathcal{A}$.

Let $\beta = \alpha - \delta$, then these public parameters are well-formed. Also note that these public parameters have a distribution identical to those in the last game. Therefore we have

$$\Pr[X_2] = \Pr[X_1]. \tag{11}$$

It is worth pointing out that, all these public parameters can be generated from $(g', g_4', g, g_1, g_2, g_4, g_5)$, without knowing the value α. Also note that the corresponding master secret key msk can be computed

without knowing the value α. To see this, let $F_2(x)$ denote the 1-degree polynomial $\frac{F_1(x)-F_1(\delta)}{x-\delta}$. Then the master secret key can be computed as $msk = g^{F_2(\alpha)}$, which can be computed from (g, g_1). Note that this is a valid master secret key as required, since $g^{F_2(\alpha)} = g^{\frac{F_1(\alpha)-F_1(\delta)}{\alpha-\delta}} = w_2^{\frac{1}{\alpha-\delta}} = w_2^{\frac{1}{\beta}}$.

Game$_3$. (Modify the challenge ciphertext) In this game, we modify **Game**$_2$ to obtain a new game. These two games are identical, except for a small modification in the encryption oracle as below: Suppose at the beginning of the Challenge stage the adversary outputs an identity $\mathsf{ID}^* = (\mathsf{ID}_1^*, \cdots, \mathsf{ID}_k^*)$. Let $F_3(x) = x^4$ and let $F_4(x) = \frac{F_3(x)-F_3(\delta)}{x-\delta}$, which is a polynomial of degree 3. Let $F_5(x) = (F_1(x) - F_1(\delta))\cdot F_4(x)$, and express $F_5(x)$ as $F_5(x) = \sum_{i=0}^{5} F_{5,i}x^i$, where $F_{5,i}$ is the coefficient of x^i in $F_5(x)$. Pick $s' \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and compute the challenge ciphertext $C^* = (C_1^*, C_2^*)$ as

$$C_1^* = g'^{s'\cdot(F_3(\alpha)-F_3(\delta))}, \quad C_2^* = C_1^{*t^*\mu+v'+\sum_{i=1}^{k} v_i\mathsf{ID}_i^*},$$

where $t^* = H(C_1^*)$. And the session key is $K_1^* = e\left(g_3, g'\right)^{s'F_{5,3}} \cdot e\left(g', \prod_{\substack{i=0\\ i\neq 3}}^{5} g_i^{s'F_{5,i}}\right)$.

At last, the simulator picks $K_0^* \overset{\$}{\leftarrow} \mathbb{G}_T$, $b \overset{\$}{\leftarrow} \{0,1\}$, and then returns the pair (K_b^*, C^*) to adversary $\mathcal{A}$.

Observe that this challenge ciphertext is well-formed as required. To see this, let $s = \left(\log_g g'\right) s'F_4(\alpha)$, then

$$\begin{aligned}
C_1^* &= g'^{s'\cdot(F_3(\alpha)-F_3(\delta))} = g^{\left(\log_g g'\right)\cdot s'\cdot(F_3(\alpha)-F_3(\delta))} = g^{\left(\log_g g'\right)\cdot s'\cdot F_4(\alpha)\cdot(\alpha-\delta)} = g^{s\cdot(\alpha-\delta)} = w_1^s,\\
C_2^* &= C_1^{*t^*\mu+v'+\sum_{i=1}^{k} v_i\mathsf{ID}_i^*} = w_1^{s\cdot(t^*\mu+v'+\sum_{i=1}^{k} v_i\mathsf{ID}_i^*)}\\
&= \left(w_1^{t^*\mu}\cdot w_1^{v'}\cdot\prod_{i=1}^{k} w_1^{v_i\mathsf{ID}_i^*}\right)^s = \left(u^{t^*}\cdot h'\prod_{i=1}^{k} h_i^{\mathsf{ID}_i^*}\right)^s,\\
K_1^* &= e\left(g', g_3\right)^{s'F_{5,3}}\cdot e\left(g', \prod_{\substack{i=0\\ i\neq 3}}^{5} g_i^{s'F_{5,i}}\right) = e\left(g', \prod_{i=0}^{5} g_i^{s'F_{5,i}}\right) = e\left(g', g\right)^{s'\sum_{i=0}^{5} F_{5,i}\alpha^i}\\
&= e\left(g, g\right)^{\left(\log_g g'\right)\cdot s'F_5(\alpha)} = e\left(g, g\right)^{\left(\log_g g'\right)\cdot s'\cdot F_4(\alpha)\cdot(F_1(\alpha)-F_1(\delta))}\\
&= \left(g, g^{F_1(\alpha)-F_1(\delta)}\right)^s = e\left(w, w_2\right)^s = Y^s.
\end{aligned}$$

Furthermore, s is indeed a random integer in $\mathbb{Z}_p^*$, since s' is a random integer in $\mathbb{Z}_p^*$. Therefore, C^* is a valid challenge ciphertext and has a distribution identical to that in the last game. Therefore, we have

$$\Pr[X_3] = \Pr[X_2]. \tag{12}$$

Game$_4$. (Again modify the challenge ciphertext) This game is identical to **Game**$_3$, except that the session key K_1^* is computed as

$$K_1^* = Z^{s'F_{5,3}}\cdot e\left(g', \prod_{\substack{i=0\\ i\neq 3}}^{5} g_i^{s'F_{5,i}}\right),$$

where Z is a random element in $\mathbb{G}_T$.

Observe that **Game**$_4$ and **Game**$_3$ are equal unless adversary $\mathcal{A}$ can distinguish $e(g', g_3)$ from a random element in $\mathbb{G}_T$. Therefore we have

$$\left|\Pr[X_4] - \Pr[X_3]\right| \leqslant \mathrm{Adv}^{2-\mathrm{MBDHE}}_{\mathcal{B},(\mathbb{G},\mathbb{G}_T)}, \tag{13}$$

for any adversary $\mathcal{B}$ against the hardness of the decisional 2-MBDHE assumption with running time

$$\mathsf{Time}_{\mathcal{B}} = \mathsf{Time}_{\mathcal{A}} + \mathcal{O}\left(l \cdot (q_e + q_d)t_{exp} + q_d \cdot t_{par}\right).$$

Game$_5$. (Replace the challenge ciphertext) We again modify encryption oracle in **Game**$_4$ to obtain a new game **Game**$_5$. Concretely, the simulator replaces the session key K_1^* in the challenge ciphertext C^* with a random element from $\mathbb{G}_T$. Note that since Z is a random element in $\mathbb{G}_T$, the session key K_1^* computed in **Game**$_4$ is also a random element in $\mathbb{G}_T$. Hence the session key computed in this game has a distribution identical to that in **Game**$_4$. Therefore, we have

$$\Pr[X_5] = \Pr[X_4]. \tag{14}$$

Furthermore, since K_1^* is completely independent of the challenge bit b, we have

$$\Pr[X_5] = \frac{1}{2}. \tag{15}$$

Inequality (7) now follows immediately from Eqs (8)–(15). This completes the proof of this theorem. □

Next, we give a comparison between our HIBKEM and other HIBKEM systems without random oracles.

Kiltz and Galindo [29] suggested a method for extending their IBKEM to a HIBKEM. Details were provided in [6]. Recently, Sarkar and Chatterjee [22] have proposed a more efficient CCA2-secure hybrid HIBE system. These systems are fully secure without random oracles under the BDDH assumption. However, the ciphertext sizes as well as the computation cost grow linearly with the hierarchy depth, and the security degrades exponentially in the hierarchy depth.

Based on Boneh-Boyen [3] and Boneh-Boyen-Goh [5] HIBE systems, Boneh et al. [11] sketched how to construct two CCA2-secure HIBKEM systems. Nevertheless, the resulting systems are secure in the selective-ID model. Kiltz [31] pointed out that, based on Waters' IBE scheme, his technique can be used to obtain a CCA2-secure HIBE. However, the ciphertext size and computation cost grow linearly with the hierarchy depth. He also argued that, using a technique from [5] it is further possible to achieve constant size ciphertext. However, the security reduction is still exponential in the hierarchy depth, and its underlying assumption (i.e., l-wDBDHI* or l-BDHE) is not fixed and becomes stronger as the hierarchy depth increases.

As to our HIBKEM scheme, the ciphertext consists of only 2 elements in $\mathbb{G}$, and the decapsulation needs only 3 pairings, independent of the identity depth. It is adaptive chosen-ciphertext secure in the full model without random oracles, and the security is tightly related to the decisional 2-MBDHE assumption. Although this assumption is non-standard, it is fixed and does not become stronger as the hierarchy depth increases.

5. Conclusions

To ensure the data confidentiality for MANETs, we presented a fully secure HIBE scheme, in which the ciphertext size and the decryption cost are constant, and the security reduction is tight, regardless of the hierarchy depth and the number of private key queries. Our proposed scheme is quite efficient, and is rather suitable for MANETs. Based on our HIBE scheme, we also proposed a direct and efficient chosen-ciphertext secure HIBKEM scheme, whose ciphertext consists of only two elements in $\mathbb{G}$, independent of the identity depth.

Acknowledgments

This work was supported by the National Science Foundation of China under Grant Nos. 61272413, 61133014, 61070249, 61272415, the Fok Ying Tung Education Foundation under Grant No. 131066, the Program for New Century Excellent Talents in University under Grant No. NCET-12-0680, the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security under Grand No. AGK2011003, and the R&D Foundation of Shenzhen Basic Research Project under Grant No. JC201105170617A.

References

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi, Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In Advanecs in Cryptology-Crypto'05, LNCS 3621, Springer-Verlag, 2005, pp. 205–222.

[2] M. Abe, R. Gennaro, K. Kurosawa and V. Shoup, Tag-KEM/DEM: A New Framework for Hybrid Encryption. In Advanecs in Cryptology-Eurocrypt 2005, LNCS 3494, Springer-Verlag, 2005, pp. 128–146.

[3] D. Boneh and X. Boyen, Efficient selective-ID secure identity-based encryption without random oracles. In Advanecs in Cryptology-Eurocrypt'04, LNCS 3027, Springer-Verlag, 2004, pp. 223–238.

[4] D. Boneh and X. Boyen, Secure identity based encryption without random oracles. In Advanecs in Cryptology-Crypto'04, LNCS 3152, Springer-Verlag, 2004, pp. 443–459.

[5] D. Boneh, X. Boyen and E.J. Goh, Hierarchical Identity Based Encryption with Constant Size Ciphertext. In Advanecs in Cryptology-Eurocrypt'05. LNCS 3494, Springer-Verlag, 2005, pp. 440–456.

[6] J. Birkett, A.W. Dent, G. Neven and J. Schuldt, Identity based key encapsulation with wildcards. Cryptology ePrint Archive, Report 2006/377, 2006. http://eprint.iacr.org/.

[7] D. Boneh and M. Franklin, Identity based encryption from the Weil pairing. In Advanecs in Cryptology-Crypto'01, LNCS 2139, Springer-Verlag, 2001, pp. 213–229.

[8] K. Bentahar, P. Farshim, J. Malone-Lee and N.P. Smart, Generic constructions of identity-based and certificateless KEMs. Cryptology ePrint Archive, Report 2005/058, 2005, http://eprint.iacr.org/.

[9] D. Boneh, C. Gentry and M. Hamburg. Space-Efficient Identity Based Encryption Without Parings. Cryptology ePrint Archive, Report 2007/177, 2007, http://eprint.iacr.org/.

[10] D. Boneh and J. Katz, Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In Proc. of CT-RSA'05, LNCS 3376, Springer-Verlag, 2005, pp. 87–103.

[11] X. Boyen, Q. Mei and B. Waters, Simple and efficient CCA2 security from IBE techniques. In Proc. of ACM CCS'05, New-York: ACM Press, 2005, pp. 320–329.

[12] X. Boyen, General Ad Hoc Encryption from Exponent Inversion IBE. In Advanecs in Cryptology-Eurocrypt'07, LNCS 4515, Springer-Verlag, 2007, pp. 394–411.

[13] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Proc. of ACM CCS'93, New York, NY, USA, 1993. ACM Press, pp. 62–73.

[14] R. Canetti and S. Goldwasser, An efficient threshold public key cryptosystem secure against adaptive chosen ciphertext attack. In Advanecs in Cryptology-Eurocrypt'99, LNCS 1592, Springer-Verlag, 1999, pp. 90–106.

[15] R. Canetti, S. Halevi and J. Katz, A Forward-Secure Public-Key Encryption Scheme. In Advanecs in Cryptology-Eurocrypt'03, LNCS 2656, Springer-Verlag, 2003, pp. 255–271.

[16] R. Canetti, S. Halevi and J. Katz, Chosen-ciphertext security from identity-based encryption. In Advanecs in Cryptology-Eurocrypt'04, LNCS 3027, Springer-Verlag, May 2004, pp. 207–222.

[17] R. Canetti, O. Goldreich and S. Halevi, The random oracle methodology, revisited, *Journal of the ACM (JACM), ACM press* **51**(4), 557–594.

[18] R. Canetti, O. Goldreich and S. Halevi, The random oracle methodology, revisited. In Proc. of STOC'98, 1998, pp. 209–218.

[19] C. Cocks, An identity based encryption scheme based on quadratic residues. In Proc. of the 8th IMA Int. Conf., 2001, pp. 26–28.

[20] R. Cramer and V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, *SIAM Journal on Computing* **33**(1) (2003), 167–226.

[21] S. Chatterjee and P. Sarkar, HIBE with Short Public Parameters Secure in the Full Model Without Random Oracles. In Advanecs in Cryptology-Asciacrypt'06, LNCS 4284, Springer-Verlag, 2006, pp. 145–160.

[22] P. Sarkar and S. Chatterjee. Construction of a Hybrid Hierarchical Identity Based Encryption Protocol Secure Against Adaptive Attack (Without Random Oracles). Cryptology ePrint Archive, Report 2006/362, 2006. http://eprint.iacr.org/.
[23] S. Chatterjee and P. Sarkar. New Constructions of Constant Size Ciphertext HIBE Without Random Oracle. In Proc. of ICISC'06, LNCS 4296, Springer-Verlag, 2006, pp. 310–327.
[24] C. Gentry, Practical identity-based encryption without random oracles. In Advanecs in Cryptology-Eurocrypt'06, LNCS 3027, Springer-Verlag, 2006, pp. 445–464.
[25] Y. Fang, X. Zhu and Y. Zhang, Securing resource-constrained wireless ad hoc networks, *Wireless Communications* **16**(2) (2009), 24–29.
[26] C. Gentry and A. Silverberg, Hierarchical ID-based cryptography. In Advanecs in Cryptology-Asiacrypt'02, LNCS 2501, Springer-Verlag, 2002, pp. 548–566.
[27] J. Horwitz and B. Lynn, Towards hierarchical identity-based encryption. In Advanecs in Cryptology-Eurocrypt'02, LNCS 2332, Springer-Verlag, 2002, pp. 466–481.
[28] K. Kurosawa and Y. Desmedt, A new paradigm of hybrid encryption scheme. In Advanecs in Cryptology-Crypto'04, LNCS 3152, Springer-Verlag, 2004, pp. 426–442.
[29] E. Kiltz and D. Galindo, Direct Chosen-Ciphertext Secure Identity-Based Key Encapsulation without Random Oracles. Cryptology ePrint Archive, Report 2006/034, 2006. http://eprint.iacr.org/.
[30] E. Kulla, M. Hiyama, M. Ikeda, L. Barolli, V. Kolici and R. Miho, MANET performance for source and destination moving scenarios considering OLSR and AODV protocols, *Mobile Information Systems* **6**(4) (2010), 325–339.
[31] E. Kiltz, Chosen-ciphertext secure identity-based encryption in the standard model with short ciphertexts. Cryptology ePrint Archive, Report 2006/122, 2006. http://eprint.iacr.org/.
[32] Y.-S. Kim, Y.-S. Shim and K.-H. Lee, A cluster-based web service discovery in MANET environments, *Mobile Information Systems* **7**(4) (2011), 299–315.
[33] B. Lynn, Authenticated Identity-Based Encryption. Cryptology ePrint Archive, Report 2002/072, 2002. http://eprint.iacr.org/.
[34] F. Mari, I. Melatti, E. Tronci and A. Finzi, A multi-hop advertising discovery and delivering protocol for multi administrative domain MANET, *Mobile Information Systems* **9**(3) (2013), 261–280.
[35] D. Naccache, Secure and practical identity-based encryption. Cryptology ePrint Archive, Report 2005/369, 2005. http://eprint.iacr.org/.
[36] V. Pham, E. Larsen, ∅. Kure and P. Engelstad, Routing of internal MANET traffic over external networks, *Mobile Information Systems* **5**(3) (2009), 291–311.
[37] P. Sarkar and S. Chatterjee, Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model. In Proc. of ICISC'05, LNCS 3935, Springer-Verlag, 2005, pp. 424–440.
[38] Secure hash standard. National Institue of Standards and Technology, NIST FIPS PUB 180-1, U.S. Department of Commerce, Apr. 1995.
[39] A. Shamir, Identity-based cryptosystems and signature schemes. In Advanecs in Cryptology-Crypto'84, LNCS 196, Springer-Verlag, 1984, pp. 47–53.
[40] B. Waters, Efficient identity-based encryption without random oracles. In Advanecs in Cryptology-Eurocrypt'05, LNCS 3494, Springer-Verlag, 2005, pp. 114–127.
[41] S. Zhao, A. Aggarwal, R. Frost and X. Bai, A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks, *IEEE Communications Surveys and Tutorials* **14**(2) (2012), 380–400.
[42] K. Zhao, L. Huang, H. Li, F. Wu, J. Chu and L. Hu, A Survey on Key Management of Identity-based Schemes in Mobile Ad Hoc Networks, *Journal of Communications* **8**(11) (2013), 768–779.
[43] Y. Zhang, W. Liu, W. Lou and Y. Fang, Securing mobile ad hoc networks with certificateless public keys, *IEEE Transactions on Dependable and Secure Computing* **3**(4) (2006), 386–399.

Kai He obtained her BS degree from Jinggangshan University in 2010, and obtained her PhD degree from Jinan University in 2012. Since 2013, she has been a PhD candidate at Jinan University in College of Information Science and Technology. Her research interests include cryptography and information security. She has published several papers in referred conferences and journals.

Min-Rong Chen obtained her BS and MS degrees from South China University of Technology in 2000 and 2004 respectively. She obtained her PhD degree from Shanghai Jiao Tong University in 2008. She came to Shenzhen University in 2008 and was appointed as an associated professor at College of Information Engineering. Her research interests includes cryptography and optimization algorithm. She has published more than 20 papers in referred conferences and journals.

Yijun Mao obtained his BS degree from Zhengzhou University in 1997, and obtained his BS Degree from South China University of Technology in 2004. Since then, he came to South China Agricultural University and was appointed as a lecture in

College of Informatics. Since 2009, he has been a PhD candidate at Sun Yat-Sen University in School of Information Science and Technology. His research interests include cryptography and information security. He has published several papers in referred conferences and journals.

Xi Zhang obtained his BS degree from Xiąfan Jiao Tong University in 1989, and obtained his BS Degree from South China University of Technology in 1997. Since then he came to Shenzhen University and was appointed as an associated professor at College of Information Engineering College of Computer Science and Software Engineering. His research interests include cryptography and information security. He has published more than 30 papers in referred conferences and journals.

Yiju Zhan obtained his BS and MS degrees from Hefei University of Technology in 1981 and 1986 respectively. He obtained his PhD Degree from Hong Kong University in 1998. He worked in Hefei University of Technology as a professor in 1998, and came to Guangdong Automation Engineering R&M Center in 1999. Since 2004, he came to Sun Yat-Sen University and was appointed as an professor in Engineering School. His research interests include information security, Control theory and application. He has published more than 50 papers in referred conferences and journals.