Fully secure hierarchical inner product encryption for privacy preserving keyword searching in cloud

Leyou Zhang and Zhuanning Wang*

School of Mathematics and Statistics,
Xidian University,
Xi’an, 710071, Shaanxi, China
Email: lyzhang@mail.xidian.edu.cn
Email: wangzhuanning0206@163.com
*Corresponding author

Yi Mu

School of Computer Science and Engineering,
University of Wollongong,
2500, Wollongong, Australia
Email: ymu@uow.edu.au

Yupu Hu

School of Telecommunications Engineering,
Xidian University,
Xi’an, 710071, Shaanxi, China
Email: yphu@mail.xidian.edu.cn

Abstract: Cloud computing provides dynamically scalable resources provisioned as a service over networks. But untrustworthy cloud service provider (CSP) offers a big obstacle for the adoption of the cloud service since CSP can access data in cloud without data owner’s permission. Hierarchical inner product encryption (HIPE) covers all applications of anonymous encryption, fully private communication and search on encrypted data, which provides trusted data access control policy to CSP. However, the existing works only achieve either selectively attribute-hiding or adaptively attribute-hiding under some strong assumptions in the public key setting. These schemes only support limited class of functions and can not protect the privacy of the query. To overcome these shortcomings, a novel HIPE in private key setting is issued. The proposed scheme achieves both fully secure and security reduction under the decisional linear (DLIN) assumption in the standard model. It has longer-size secret keys and size ciphertexts and brings the high computational complexity. Therefore, a variant of the basic scheme is presented with the same security but shorter ciphertexts.

Keywords: cloud security; searching encryption; hierarchical inner product encryption; HIPE; the DLIN assumption.


Biographical notes: Leyou Zhang received his PhD from the Xidian University in 2009. Currently, he is an Associate Professor in the Department of Mathematical Science of Xidian University. His current research interests include network security, computer security, and cryptography. He has published more than 70 papers in international and domestic journals and conferences.

Zhuanning Wang is a Master candidate. Her main research interest includes computer security, and public key cryptography.

Yi Mu received his PhD from the Australian National University in 1994. He is currently a Professor, Head of School of Computer Science and Software Engineering and the co-Director of Centre for Computer and Information Security Research at University of Wollongong, Australia. His current research interests include network security, computer security, and cryptography. He is the Editor-in-Chief of International Journal of Applied Cryptography and serves as an Associate Editor for nine other international journals. He is a senior member of the IEEE and a member of the IACR.

Copyright © 2018 Inderscience Enterprises Ltd.
1 Introduction

Cloud computing, a new computing paradigm, provides dynamically high-quality cloud-based services and applications over the internet. The cloud storage-based information retrieval service is a promising technology that will form a vigorous market. The cloud storage (service) providers are responsible for keeping the data available and accessible, and the physical environment protected and running. However, CSP is an authorized controller and access the data in anytime and anywhere without owner’s permission. Hence the security and privacy protection are issued in cloud. Cryptographic method is considered at first. The contents are encrypted before storage in cloud. But the general encryption would not be suitable for cloud information retrieval systems because the CSP cannot retrieve encrypted contents from a plaintext query without the decryption private key. So the searching encryption is introduced in Boneh et al. (2004). In this scheme, the entity performing the retrieval service is not allowed to learn the content of the queries and responses. And some additional encrypted index terms (serving as keywords) are used for the data search process. Recently, there are some schemes proposed in cloud, such as Benamara and Li (2015), Dutu et al. (2014), Ye and Khoussainov (2013), and Thabet et al. (2014).

Functional encryption (FE) (Boneh et al., 2011) is an advanced encryption and covers almost all typical encryption schemes, such as identity-based encryption (IBE) (Boneh and Franklin, 2001; Luo, 2015; Luo and Chen 2014), attribute-based encryption (ABE) (Nishide et al., 2008; Wang and Li, 2013), hidden vector encryption (HVE) (Shi and Waters, 2008), inner-product encryption (IPE) (Park, 2011). The relation $R(\bar{v}, \bar{x})$ in this scheme determines how to decrypt a ciphertext under parameter $\bar{x}$ with a secret key under parameter $\bar{v}$. Generally, attribute-hiding FE is called predicate encryption (PE) in Katz et al. (2008). Recently, a strong security notion for PE is introduced in Katz et al. (2008), which is called attribute-hiding. Under this encryption system, a ciphertext conceals all attributes as well as the plaintext. PE for IPE is a new way of viewing encryption which opens up a much larger world of possibilities for sharing encrypted data, such as Attrapadung and Libert (2010), Lewko et al. (2010) and Okamoto and Takashima (2009a, 2009b, 2010, 2011, 2012). In an IPE system, a relation $R(\bar{v}, \bar{x})$ holds if $\bar{x} \cdot \bar{v} = 0$. The advanced functionality and flexibility provided by such systems is very appealing for many practical applications.

There are two security notions for attribute-hiding FE, fully attribute-hiding and selectively attribute-hiding. In the fully attribute-hiding definition (Okamoto and Takashima, 2012), adversary $\mathcal{A}$ is allowed to ask a key-query for $\bar{v}$ such that $\bar{v} \cdot \bar{x}^{(0)} = \bar{v} \cdot \bar{x}^{(1)} = 0$ provided that $(m^{(0)}, m^{(1)})$ ($\bar{x}^{(0)}$ and $m^{(b)}, b \in \{0,1\}$) are for the challenge ciphertext in the security definition). But in selectively attribute-hiding security definition (Okamoto and Takashima, 2009a), $\mathcal{A}$ is only allowed to ask a key-query for $\bar{v}$ such that $\bar{v} \cdot \bar{x}^{(b)} \neq 0$ for all $b \in \{0, 1\}$. In addition, it also supports delegation computation. Katz et al. (2008) gave an expressive attribute-hiding PE but no delegation mechanism. Okamoto and Takashima (2009b) introduced a new construction of hierarchical inner product encryption (HIPE) but the security proof was only given in the generic model. Okamoto and Takashima (2009a) proposed the first HIPE scheme that was selectively attribute-hiding security in the standard model under the RDSP and IDSP assumptions. After that, an efficient HIPE scheme was presented in Lewko et al. (2010), but the security was still proved in the selective model. More recently, Okamoto and Takashima (2012) presented a HIPE scheme that achieves full security under the standard d-linear assumption on prime order bilinear groups. However, they required that secret every subspace base with increasing the parameters and bringing a large amount of computational cost. It is a technically challenging task to achieve an adaptively secure and fully attribute-hiding HIPE scheme. Most recent constructions were issued from lattice (Abdalla et al., 2012; Hou et al., 2014), but both schemes are selectively attribute-hiding security in the public key setting.

1.1 Our contribution

Our primary goal is to construct a scheme that hides both attributes and predicates supporting inner-products in the private key setting. Motivated by the above challenge, we propose a fully secure HIPE scheme in the private key setting under the decisional linear (DLIN) assumption. To achieve this point, we combine the techniques in Lewko et al. (2010) and Okamoto and Takashima (2010, 2012). Note that the vector space consists of four orthogonal subspaces, i.e., real encoding part, hidden part, secret-key randomness part and ciphertext randomness part. The proof...
employs a hybrid argument over a sequence of security games, which have been used in Lewko and Waters (2010) and Agrawal et al. (2013). Considering the longer ($O(n)$-size) ciphertexts and ($O(l)$-size) secret keys in the basic one, we presented a new scheme with the same security which achieves shorter ($O(1)$-size) ciphertexts.

1.2 Application of HIPE

With the development of cloud computing, and more and more data stored in the cloud server, how to find a specific file in a large number of documents has become a challenge, because the predicate encryption is suitable for data access control system and achieves the retrieval of encrypted data in cloud. Therefore, our system can be used for file retrieval systems. We give a specific application as shown in Figure 1.

First, the data providers need to extract attribute vectors from the file to generate tokens and generate an encrypted file which is stored in the cloud service. When the file is used by data retrievers, only the predicate vector is provided to the server, and the server is calculated predicate $f$ with attribute vectors $\vec{x}$ and predicate attribute vectors $\vec{v}$. The server sends encrypted files to data retrievers iff $\vec{x} \cdot \vec{v} = 0$, otherwise, output special symbols ⊥.

New system can distribute the private key to the lower level files through the superior one to avoid the leakage of the circulation. Furthermore, its security can also guarantee the privacy of the file and the privacy of the retrieval, which is more natural than those already available.

2 Preliminaries

2.1 The DLIN assumption

Definition 1: The DLIN problem (Okamoto and Takashima, 2012) is to guess $\beta \in \{0,1\}$ given

$$(\text{param}_{\beta}, G, \xi G, \kappa G, \delta G, \sigma G) \leftarrow \text{G}_{\beta\text{DLIN}}(1^\lambda),$$

where

$\text{G}_{\beta\text{DLIN}}(1^\lambda): \text{param}_{\beta} := (g, G, G_T, G, e) \leftarrow \text{G}_{\beta\text{pbg}}(1^\lambda),$

$\kappa, \delta, \xi, \sigma \leftarrow \mathbb{F}_q,$

$Y_0 := (\delta + \sigma) G, Y_1 \leftarrow \mathbb{G},$

return

$$(\text{param}_{\beta}, G, \xi G, \kappa G, \delta G, \sigma G, Y_\beta) \leftarrow \text{G}_{\beta\text{DLIN}}(1^\lambda),$$

for $\beta \leftarrow \mathbb{U}\{0,1\}.$

For a probabilistic machine $\varepsilon$, the advantage of $\varepsilon$ for the DLIN problem is defined as:

$$\text{Adv}^\lambda_{\varepsilon} := |\text{Pr}[\varepsilon(1^\lambda, \rho) \rightarrow 1] - \text{Pr}[\varepsilon(1^\lambda, \rho) \rightarrow 1]|.$$

The DLIN assumption holds if for any probabilistic polynomial-time adversary $\varepsilon$, the advantage $\text{Adv}^\lambda_{\varepsilon}(\lambda)$ is negligible in $\lambda$.

2.2 Definition of private key HIPE

$\vec{n} := (n, d; n_1, \ldots, n_d)$ are positive integers with

$n_0 = 0 < n_1 < n_2 < \ldots < n_d = n$. Let $\sum_i := \mathbb{F}_q^{n_i-n_{i-1}} \setminus \{0\}$ be the sets of attributes, where each $\sum_i := \mathbb{F}_q^{n_i-n_{i-1}} \setminus \{0\}$. $\sum := \bigcup_{i=1}^d (\sum_i \times \ldots \times \sum_i)$ is the hierarchical attributes, where the union is a disjoint union. Then, for $\vec{v}_i \in \mathbb{F}_q^{n_i-n_{i-1}} \setminus \{0\}$, the hierarchical predicate $f_{\vec{v}_1, \ldots, \vec{v}_d}$ on hierarchical attributes $(\vec{x}_1, \ldots, \vec{x}_k)$ is defined as follows: $f_{\vec{v}_1, \ldots, \vec{v}_d}(\vec{x}_1, \ldots, \vec{x}_k) = 1$ iff $\vec{x}_i \cdot \vec{v}_i = 0$ for all $i$ s.t., $1 \leq i \leq d$. 
Definition 2: A private key HIPE (HIPE_{priv}) scheme for the class of hierarchical inner-product predicates over the set of hierarchical attribute Σ consists of probabilistic polynomial-time algorithms Setup, KeyGen, Enc, Dec and Delegate, for ℓ = 1, ..., d. They are given as follows:

- **Setup:** This algorithm takes as input security parameter 1^λ and format of hierarchy n, and outputs (master) secret key sk.
- **KeyGen:** This algorithm takes as input the master secret key sk and predicate vectors v := (v_1, ..., v_i). It outputs a corresponding secret key k^{v_1}_{v_1}.
- **Enc:** This algorithm takes as input the master secret key sk, attribute vectors x := (x_1, ..., x_i) and plaintext m in some associated plaintext space, M. It returns ciphertext C_x.
- **Dec:** This algorithm takes as input secret key k^{v_1}_{v_1}, where 1 ≤ ℓ ≤ d, and ciphertext C_x. It outputs either plaintext m or the distinguished symbol ⊥.
- **Delegate:** This algorithm takes as input the master secret key sk, ℓth level secret key k^{v_1}_{v_1}, and ℓ + 1th level secret vector v_1 and returns ℓ + 1th level secret key k^{v_1}_{v_1}.

2.3 Security model

The full security in the private-key setting is similar to the adaptively attribute-hiding security model in the public-key setting as defined follows (Okamoto and Takashima, 2012).

1. **Setup:** is run to generate keys sk.

2. A may adaptively makes a polynomial number of queries of the following type: A asks the challenger to an key for predicate v^{(0)}, v^{(1)}.

   In response, A is given the corresponding key, where b ∈ {0, 1},

   k^{v^{(b)}}_{v^{(b)}} ← R KeyGen(sk, v^{(b)} := (v_1^{(b)}, ..., v_i^{(b)})).

3. A outputs challenge attribute vector x^{(0)}, x^{(1)}, where x^{(0)} := (x_1^{(0)}, ..., x_i^{(0)}), x^{(1)} := (x_1^{(1)}, ..., x_i^{(1)}), and challenge plaintexts (m^{(0)}, m^{(1)}) subject to the following restrictions:
   a. v · x^{(0)} ≠ 0 and v · x^{(1)} ≠ 0 for all the queried predicate vectors.
   b. Two challenge plaintexts are equal, m^{(0)}, m^{(1)}, i.e., one of the following conditions.
      • v · x^{(0)} = 0 and v · x^{(1)} = 0
      • v · x^{(0)} ≠ 0 and v · x^{(1)} ≠ 0.

A random bit b is chosen. A is given

C_x^{(b)} ← R Enc(sk, m^{(b)}, x^{(b)}).

4. The adversary may continue to request keys for additional predicate vectors subject to the restrictions given in challenge. A is given the corresponding key

k^{v_1}_{v_1} ← R KeyGen(sk, v := (v_1, ..., v_i)).

5. A outputs a bit b′, and succeeds if b′ = b. We define the advantage of A as

Adv_A^{HIPE_{priv}}(λ) := Pr[b′ = b] - 1/2.

3 New constructions

In the description of the scheme, we assume that the first coordinate, x_1, of input vector, x := (x_1, ..., x_n), is non-zero.

- **Setup:** (1^λ, n := (d; n_1, ..., n_d)):

  (param_{G}, {B_j, B'_j}_{j=0,...,d}) ← R G_0(1^λ, n),

  B_0 := (b_0, ..., b_{d,5n}), B_i := (b_i, ..., b_{i,5n}),

  B_0 := (b_0, ..., b_{i,5n}), B_i := (b_i, ..., b_{i,5n}),

  for t = 1, ..., d, sk := (B, B'_t)_{t=0,...,d}, return sk.

- **KeyGen:**

  (sk, (v_1, ..., v_i)) := ((v_1, ..., v_n), (v_{n+1}, ..., v_{n}),)

  for

  t = 1, ..., d, η_{dec_{t}}, s_{dec_{t}}, θ_{dec_{t}}, θ_{dec_{t}} ← U S_{dec},

  η_{ran_{t}}, s_{ran_{t}}, θ_{ran_{t}}, θ_{ran_{t}} ← U S_{ran},

  k^{v_1}_{v_1} := (−s_{dec_{t,0}}), s_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}} ∈ B^n,

  k^{v_1}_{v_1} := (s_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}) ∈ B^n,

  k^{v_1}_{v_1} := (s_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}) ∈ B^n,

  k^{v_1}_{v_1} := (s_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}, η_{dec_{t,0}}, θ_{dec_{t,0}}) ∈ B^n,

  return

  k^{v_1}_{v_1} := (k^{v_1}_{v_1}, k^{v_1}_{v_1}, (k^{v_1}_{v_1}),)_{n_{a,c}, ..., n_y},

  k^{v_1}_{v_1} := (k^{v_1}_{v_1}, k^{v_1}_{v_1}, (k^{v_1}_{v_1}),)_{n_{a,c}, ..., n_y}.

- **Enc:**

  (sk, m ∈ G_T, x := (x_1, ..., x_i)) := ((x_1, ..., x_n), ..., (x_{n+1}, ..., x_n)).
Theorem 1: The scheme \( \text{HIPE}_0 \) described above is a single challenge IND secure public-key HIPE scheme under the DLIN assumption.

Proof: Following Okamoto and Takashima’s (2012) approach, we construct the same number of hybrids in the same way, where the only difference is that our ciphertexts and keys have some extra elements at the end. Then, we will show how the DLIN assumption can be reduced to both Problem 1 and Problem 2 via Basic Problem 0 defined in Okamoto and Takashima (2010), where they also show how the DLIN assumption is reduced to this problem.

Problem 1: Let

\[
\{ \text{param}_a, \{ \mathbf{B}_0, \mathbf{B}_1 \}_{i=0, \ldots, d}, f_{b, 0} \} \xleftarrow{\text{U}} \mathcal{G}_b(1^k, \tilde{n}),
\]

where

\[
\mathcal{G}_b(1^k, \tilde{n}) := \langle d; n_0, \ldots, n_d \rangle.
\]

\[
\{ \text{param}_a, \{ \hat{\mathbf{B}}_0, \hat{\mathbf{B}}_1 \}_{i=0, \ldots, d}, f_{b, 0} \} \xleftarrow{\text{U}} \mathcal{G}_b(1^k, \tilde{n}),
\]

in an experiment \( \exp(\cdot) \) and is supposed to guess \( b \). The advantage in Problem 1 is defined as:

\[
\text{Adv}_{\text{atk}, 1}(\lambda) = | \Pr[\exp(0)| (1^k) = 1] - \Pr[\exp(1)| (1^k) = 1] |.
\]

Problem 2:

Let

\[
\{ \text{param}_a, \{ \mathbf{B}_0, \mathbf{B}_1 \}_{i=0, \ldots, d}, \mathbf{h}_0, \mathbf{h}_1 \} \xleftarrow{\text{U}} \mathcal{G}_b(1^k, \tilde{n}),
\]

where

\[
\mathcal{G}_b(1^k, \tilde{n}) := \langle d; n_0, \ldots, n_d \rangle.
\]

for \( t = 1, \ldots, d, t = 1, \ldots, n_t \),

\[
\{ \text{param}_a, \{ \mathbf{B}_0, \mathbf{B}_1 \}_{i=0, \ldots, d} \} \xleftarrow{\text{U}} \mathcal{G}_b(1^k, \tilde{n}),
\]

\[
\mathbf{b}_0 := (b_{0, 0}, b_{0, 0}, \ldots, b_{0, 0}, b_{0, 1}, \ldots, b_{0, n_0}),
\]

\[
\mathbf{b}_1 := (b_{1, 0}, b_{1, 0}, \ldots, b_{1, 0}, b_{1, n_0 + 1}, \ldots, b_{1, n_0 + 1}),
\]

\[
\mathbf{h}_0 := (h_0, h_0, \ldots, h_0), \mathbf{h}_1 := (h_1, h_1, \ldots, h_1),
\]

\[
\delta, \delta_0, w \xleftarrow{\text{U}} \mathbb{F}_p, \tau, \sigma \xleftarrow{\text{U}} \mathbb{F}_q.
\]
\[\tilde{e}_{i,j} = (0^{i-1},1,0^{n-i})^T \in \mathbb{F}_q^m,\]

\[h_{0,0}^0 = (\delta,0,0,0,0)_\mathbb{F}_q^m, \quad h_{i,j}^0 = (\delta,\tau,0,\delta,0)_\mathbb{F}_q^m, \quad h_{0,0}^1 = (\delta\tilde{e}_{i,j},0^0,0,\delta\tilde{e}_{i,j},0^0)_\mathbb{F}_q^m, \quad h_{i,j}^1 = (\delta\tilde{e}_{i,j},\tau\tilde{e}_{i,j},0^0,0,\delta\tilde{e}_{i,j},0^0)_\mathbb{F}_q^m, \quad h_0 = (w,\sigma,0,0,0)_\mathbb{F}_q^m, \quad h_j = (w\tilde{e}_{i,j},\sigma\tilde{e}_{i,j},0^0,0^0,0^0)_\mathbb{F}_q^m.\]

For a p.p.t. adversary, he/she is given

\[(\text{param}, \{h, \tilde{h}^j\})_{i=0,\ldots,d}, \{h_0, h_1, \{h_i,j, h_{i,j}\}_{i=0,\ldots,d;i=0,\ldots,d}; \lambda\)\]

in an experiment \(\exp^{(0)}_{h,A}\) and is supposed to guess \(b\). The advantage in Problem 2 is defined as:

\[\text{Adv}_{h,A}(\lambda) = \Pr[\exp^{(0)}_{h,A}(1^4) = 1] - \Pr[\exp^{(1)}_{h,A}(1^4) = 1].\]

In the following, we show how basic problem 0 reduces to problems 1 and 2 defined above.

**Reducing basic Problem 0 to Problem 1**: Suppose we have the following instance of problem 0:

\[(\text{param}_h, \{h, \tilde{h}^j\})_{i=0,\ldots,d}, \{h_0, h_1, \{h_i,j, h_{i,j}\}_{i=0,\ldots,d;i=0,\ldots,d}; g, \kappa G, \xi G, \delta G\}).\]

By using \(\text{param}_g = (q, \mathbb{G}, \mathbb{G}_T, G,e)\) underlying \(\text{param}_h\), we can calculate

\[\text{param}_0 = (q, \mathbb{V}, \mathbb{G}_T, A_0,e) = G_{\text{g}^{\mathbb{g}_0}}(1^4,5, \text{param}_g), \quad \text{param}_1 = (q, \mathbb{V}, \mathbb{G}_T, A,e) = G_{\text{g}^{\mathbb{g}_1}}(1^4,5n, \text{param}_g), \quad \text{param}_h = (\{\text{param}_i\}_{i=0,\ldots,d}; G_T).\]

Define the matrices \(\mathbb{D}_i = \{d_{i,1}, d_{i,2}, \ldots, d_{i,5n}\}\) and \(\mathbb{D}^*_i = \{d^*_{i,1}, d^*_{i,2}, \ldots, d^*_{i,5n}\}\) as follows:

\[d_{0,i} := \begin{cases} W_0(b^i_0,0,0), & i = 1 \\ W_0(0,0,0,0,\xi G,0), & i = 2 \\ W_0(b^i_0,0,0), & i = 3 \\ W_0(0,0,0,0,\xi G,0), & i = 4 \\ (W_{i+1}^T(b^i_0,0,0),i = 5 \end{cases}, \quad d^*_{0,i} := \begin{cases} (W_{i+1}^T(b^i_0,0,0),i = 1 \\ (W_{i+1}^T(b^i_0,0,0),i = 2 \\ (W_{i+1}^T(b^i_0,0,0,\xi G,0),i = 3 \\ (W_{i+1}^T(b^i_0,0,0),i = 4 \\ (W_{i+1}^T(0,0,0,0,\xi G,0),i = 5 \end{cases}.\]

Let \(\mathbb{D}_i = (d_{0,i}, d_{0,3}, d_{0,4}, d_{0,5})\) and \(\mathbb{D}^*_i = (d^*_{i,1}, d^*_{i,2}, \ldots, d^*_{i,5n})\).

Observe that \(\mathbb{D}_i\) and \(\mathbb{D}^*_i\) can be computed from the knowledge of \(\tilde{h}^j\) and \(\tilde{h}^j\), which are part of the given instance. Further, choose \(n-1\) numbers \(\gamma_2, \ldots, \gamma_n\) uniformly at random from \(\mathbb{F}_q\) and set the following, for \(t = 1, \ldots, d:\)

\[g_{0,0} := (\delta, 0, 0, 0, 0, 0)^\gamma_{\mathbb{g}_0}, \quad g_{0,i} := (\delta, 0, 0, 0, 0, 0)^\gamma_{\mathbb{g}_0}, \quad g_{0,0} := (\delta, 0, 0, 0, 0, 0)^\gamma_{\mathbb{g}_0}, \quad g_{1,i+1} := (\delta, 0, 0, 0, 0, 0)^\gamma_{\mathbb{g}_0}, \quad g_{1,i+1} := (\delta, 0, 0, 0, 0, 0)^\gamma_{\mathbb{g}_0}, \quad g_{i} := \delta b_j,\]

where \(\gamma := (\sigma, \gamma_2, \ldots, \gamma_n)\).

**Reducing basic Problem 0 to Problem 2**: Suppose we have the following instance of problem 0:

\[(\text{param}_h, \{h, \tilde{h}^j\})_{i=0,\ldots,d}, \{h_0, h_1, \{h_i,j, h_{i,j}\}_{i=0,\ldots,d;i=0,\ldots,d}; g, \kappa G, \xi G, \delta G\}).\]

By using \(\text{param}_g = (q, \mathbb{G}, \mathbb{G}_T, G,e)\) underlying \(\text{param}_h\), we can calculate

\[\text{param}_0 = (q, \mathbb{V}, \mathbb{G}_T, A_0,e) = G_{\text{g}^{\mathbb{g}_0}}(1^4,5, \text{param}_g), \quad \text{param}_1 = (q, \mathbb{V}, \mathbb{G}_T, A,e) = G_{\text{g}^{\mathbb{g}_1}}(1^4,5n, \text{param}_g), \quad \text{param}_h = (\{\text{param}_i\}_{i=0,\ldots,d}; G_T).\]

Let \(W_i\) be a \(5n \times 5n\) matrix on \(\mathbb{V}(t = 0, \ldots, d)\). Define the matrices \(\mathbb{D}_i := (d_{i,1}, d_{i,3}, d_{i,4}, d_{i,5})\) and \(\mathbb{D}^*_i := (d^*_{i,1}, d^*_{i,2}, d^*_{i,3}, d^*_{i,4}, d^*_{i,5})\) as follows:
Consider another public-key HIPE scheme HIPE_1 obtained
by swapping the public and private key in HIPE_0, i.e.,
\[
\text{HIPE}_1.pk = \text{HIPE}_0.msk \quad \text{and} \quad \text{HIPE}_1.msk = \text{HIPE}_0.pk,
\]
\[
\text{HIPE}_1.\text{KeyGen} = \text{HIPE}_0.\text{Enc} \quad \text{and}
\]
\[
\text{HIPE}_1.\text{Enc} = \text{HIPE}_0.\text{KeyGen}.
\]

The security of HIPE_1 follows from the security of HIPE_0
due to the symmetric nature of HIPE_{prv}.

**Lemma 2:** The scheme HIPE_1 described above is a single
challenge IND secure public-key HIPE scheme under the
DLIN assumption.

**Lemma 3:** The scheme HIPE_{prv} described above is a single
challenge IND secure public-key HIPE scheme under the
DLIN assumption.

Because Shen et al. (2009) describe how to construct a fully
secure predicate encryption scheme supporting
inner-products over vectors of length \( n \) from a single
challenge secure scheme supporting inner-products over vectors of length \( 2n \) in Shen et al. (2009). We adopt the
same approach to obtain a fully secure scheme HIPE_{prv}.

### 3.2 A variant of the proposed scheme

A variant of the proposed HIPE_{prv} is proposed in this
section. It achieves the same security as the above one and a shorter
ciphertext than the first one. We assume that input vector,
\((\tilde{x}_1, \ldots, \tilde{x}_l)\) has an index \( \ell \) \((1 \leq \ell \leq n_i - 1)\) with
\( \tilde{x}_\ell \neq \tilde{0} \), and that input vector, \((\tilde{v}_1, \ldots, \tilde{v}_j)\), satisfies \( \tilde{v}_n \neq \tilde{0} \).

Note that the random dual orthonormal basis generator
\( G^{(1)}_{\text{ob}} \) is similar to Okamoto and Takashima (2011), where
\( N_i := 5n_r \).

- **Setup** \((1^d, \tilde{n} := (d; n_1, \ldots, n_d))\):
  
  \[
  \begin{align*}
  &\text{(param}_{d}, \{B_{j}, \tilde{B}_j\}_{t=0, \ldots, d}) = \text{setup}\left(1^d, \tilde{n}\right), \\
  &\text{B}_0 := \{b_{0,1}, \ldots, b_{0,n}\}, \quad \text{B}_0 := \{b_{0,1}, b_{0,5}\}, \\
  &\text{B}_0 := \{b_{0}, \ldots, b_{n}\}, \quad \text{B}_0 := \{b_{0}, \ldots, b_{5}\}, \\
  &\text{B}_0 := \{b_{0}, \ldots, b_{n}\}, \\
  &\text{B}_0 := \{b_{0}, \ldots, b_{n}\},
  \end{align*}
  \]

  return \( sk \).

- **KeyGen** \((sk, (v_1, \ldots, v_j) := ((v_1, \ldots, v_n), (v_{n+1}, \ldots, v_{n+d}))\):

  for \( t = 1, \ldots, d \),

  \[
  \begin{align*}
  &\text{\eta}_{dec, 0}, \eta_{dec, j} \quad \leftrightarrow \quad \text{F}_Q, \quad \text{dec, 0} = \sum_{t=1}^d s_{dec, t} \\
  &\text{\theta}_{dec, 0}, \theta_{dec, j} \quad \leftrightarrow \quad \text{F}_Q(j = n_{t+1}, \ldots, n_t), \\
  &\text{\theta}_{dec, 0}, \theta_{dec, j} \quad \leftrightarrow \quad \text{F}_Q(j = 1, \ldots, \ell + 1)
  \end{align*}
  \]

Consider another public-key HIPE scheme HIPE_{1,1} obtained
by swapping the public and private key in HIPE_{0,1}, i.e.,
\[
\text{HIPE}_{1,1} \text{pk} = \text{HIPE}_{0,1} \text{msk}
\quad \text{and} \quad
\text{HIPE}_{1,1} \text{msk} = \text{HIPE}_{0,1} \text{pk},
\]
\[
\text{HIPE}_{1,1} \text{KeyGen} = \text{HIPE}_{0,1} \text{Enc} \quad \text{and}
\]
\[
\text{HIPE}_{1,1} \text{Enc} = \text{HIPE}_{0,1} \text{KeyGen}.
\]
$k_{\text{dec,0}}^{\gamma} := (-x_{\text{dec,0}}, 0, 1, \eta_{\text{dec,0}}, 0)_{\mathbb{G}_2}$,

$k_{\text{dec}}^{\gamma} := (x_{\text{dec}}, \bar{x}_1 + \theta_{\text{dec}}, \bar{V}_1, 0^n_\text{dec,1}, \bar{V}_1, 0^n_\text{dec,0})_{\mathbb{G}_2}$,

$k_{\text{del,j}}^{\gamma} := (\theta_{\text{del,j}}, \bar{V}_j, 0^n_\text{del,j}, \bar{V}_j, 0^n_\text{del,j})_{\mathbb{G}_2}$, \quad j = n_1 + \ldots, n_i,

$k_{\text{ran,j}}^{\gamma} := (\theta_{\text{ran,j}}, \bar{V}_j, 0^n_\text{ran,j}, \bar{V}_j, 0^n_\text{ran,j})_{\mathbb{G}_2}$, \quad j = 1, \ldots, \ell + 1.

return $k_{\text{dec}}^{\gamma} := (k_{\text{dec,0}}^{\gamma}, k_{\text{dec}}^{\gamma}, \{k_{\text{del,j}}^{\gamma}\}_{j=n_1+\ldots,n_i}, \{k_{\text{ran,j}}^{\gamma}\}_{j=1,\ldots,\ell+1})$.

- **Enc**

  $(sk, m \in \mathbb{G}_\ell, (\bar{x}_1, \ldots, \bar{x}_\ell) := ((x_1, \ldots, x_n), \ldots, (x_{n_1+\ldots+n_i}, \ldots, x_{\ell+1, \ldots}))$:

  $w, \zeta, \phi_0 \leftarrow \mathcal{U}_{\mathbb{F}_q^{m\times n}} \times \ldots \times \mathcal{U}_{\mathbb{F}_q^{m-n\times i}}$,

  $c_0 := (w, 0, \zeta, 0, \phi_0)_{\mathbb{G}_0}$,

  $C_{1,j} := wB_{1,j} + \eta B_{2,j} + \sigma_2 := g^{\zeta} m$,

  $C_{2,j} := \sum_{l=1}^{n_i} x_l (wB_{l,j} + \eta B_{2,j})$, \quad j = 1, \ldots, 5.

  return $C := (c_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,5}, \sigma_2)$.

- **Dec** ($C^\gamma, k_{\text{dec}}^{\gamma}$): Parse $k_{\text{dec}}^{\gamma}$ as a 5$n_i$-tuple

  $(K_{\text{dec}}^{\gamma}, K_{\text{ran}}^{\gamma}) \in \mathbb{F}_q^{5n_i}$,

  $D_j := \sum_{l=1}^{n_i} x_l K_{\text{dec}}^{\gamma}(l, j)$,

  $F := e(c_0, K_{\text{dec,0}}^{\gamma}) \prod_{j=1}^{5} e(C_{1,j}, D_j) : e(C_{2,j}, D_{\text{prv}})$.

  return $m' := \sigma_2 / F$.

- **Delegate** ($sk, k_{\text{dec}}^{\gamma}, \bar{v}_{\text{ran}} := (v_{n_1+\ldots,n_i})$):

  $\alpha_{\text{dec,j}}, \alpha_{\text{del,j}}, \sigma_{\text{del,j}}$

  $\quad (j = n_1 + \ldots, n_i), \alpha_{\text{ran,j}}$

  $\quad \sigma_{\text{ran,j}}(j = 1, \ldots, \ell + 1), \sigma_{\text{dec}}, \psi' \leftarrow \mathcal{U}_{\mathbb{F}_q}$.

Remark 1: A part of output of setup $(1^\ell, \bar{n}), \{B_{l,j}, B_{l,j}^{1,5}, 1, \ldots, 5, 1, \ldots, n_i \}$ is defined with $\mathbb{B}_l := (b_1, \ldots, b_{5n_i})_{l=0,\ldots,d}$. Decryption can be alternatively described as:

$\text{Dec}'(k_{\text{dec}}^{\gamma}, C^\gamma)$:

$\quad c_1 := (x_1C_{1,1}, \ldots, x_{n_1}C_{1,1}, C_{2,1}, \ldots, x_{n_1}C_{1,5}, \ldots, x_{n_i}C_{1,5}, C_{2,5})$,

that is,

$\quad c_1 := (w\bar{x}, 0^n_\text{dec,0}, \eta, \bar{x})_{\mathbb{G}_2}$,

$\quad F := e(c_0, K_{\text{dec,0}}^\gamma) \cdot e(c_1, k_{\text{dec}}^\gamma)$.

return $m' := c_2 / F$.

Theorem 2: The new HIPE$_{\text{prv}}$ scheme is fully secure against chosen plaintext attacks under DLIN assumption.

Theorem 2 can be proved to be similar to the Theorem 1.

### Table 1 Efficiency comparison of schemes

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Dimension of $\mathbb{V}$</th>
<th>Security</th>
<th>Assumption</th>
<th>PK</th>
<th>SK</th>
<th>CT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lewko et al. (2010)</td>
<td>2$n + 3$</td>
<td>Weak-AH</td>
<td>n-eDDH</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Okamoto and Takashima (2012)</td>
<td>4$n + d + 5$</td>
<td>Full-AH</td>
<td>DLIN</td>
<td>$O(n)$</td>
<td>$O(n)$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Ours (basic)</td>
<td>$5 + 5 \sum_{i=1}^{d} n_i$</td>
<td>Full-AH</td>
<td>DLIN</td>
<td>$O(1)$</td>
<td>$O(1)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>Ours (modified)</td>
<td>$5 + 5 \sum_{i=1}^{d} n_i$</td>
<td>Full-AH</td>
<td>DLIN</td>
<td>$O(1)$</td>
<td>$O(1)$</td>
<td>$O(1)$</td>
</tr>
</tbody>
</table>
3.3 Efficiency analysis
In this section, we first compare the proposed HIPE with some existing schemes (Lewko et al., 2010; 2012) as shown in Table 1. First, ours has high dimension of V. The schemes proposed in Okamoto and Takashima (2012) and ours (basic, modified) achieves fully attribute-hiding under the DLIN assumption, while the scheme in Lewko et al. (2010) only has weak attribute-hiding under the n-extended decisional Diffie-Hellman assumption. Second, the hierarchical technique is used in those schemes. The schemes proposed in Lewko et al. (2010) obtain $O(n^2)$ size public keys and secret keys, in Okamoto and Takashima (2012) obtain $O(n)$ size public keys and secret keys, while ours achieve $O(1)$ size public keys and $O(n)$ size secret keys. In addition, ours (modified) achieves $O(n)$ size ciphertexts, while others achieves $O(n)$ size. Therefore, the new schemes have obvious improvement in efficiency.

4 Conclusions
In this paper, two private key HIPE are proposed. The first one achieves full security and security reduction under the natural assumption-DLIN assumption in the standard model. In addition, it has shorter public/private secret keys than the existing works. However, the ciphertexts achieves $O(n)$ size. Hence the second one is proposed. It achieves constant size ciphertexts and keeps the same features as first one. For the future the research of the inner encryption on lattice has important significance.

Acknowledgements
This work was supported in part by the Nature Science Foundation of China under Grant (61472307, 61100165, 61100231), Natural Science Foundation of Shaanxi Province (2014MJ8313, 2012JQ8044, 2010JQ8004), Foundation of Education Department of Shanxi Province (2013JK1096, 2013JK0589) and the Fundamental Research Funds for the Central Universities of China and CSC Funds.

References


