論文 / 著書情報
Article / Book Information

Title	Blind HIBE and its Application to Blind Decryption
Authors	Wakaha Ogata, Phong Le Trieu
出典 / Citation	SCIS2008, Vol. , No. , pp. 4D1-2
発行日 / Pub. date	2008, 1
URL	http://search.ieice.org/
権利情報 / Copyright	本著作物の著作権は電子情報通信学会に帰属します。 Copyright (c) 2008 Institute of Electronics, Information and Communication Engineers.

SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

Blind HIBE and its Application to Blind Decryption

Le Trieu Phong * Wakaha Ogata *

Abstract— Consider the following situation: over the Internet, a company owns a chain of retailers who sell digital information (e.g., music, magazine) using their websites. The information is available in encrypted form, namely ciphertexts, on the websites. A buyer, after browsing the summaries, must pay some money to have its choice of ciphertexts decrypted by the corresponding retailers. The problem is: the buyer wishes to hide its choice of purchases (blind decryption), while the company and retailers want to make sure that the buyer cannot get more than what he/she pays. We propose a novel mechanism to solve the above problem. Additionally, it can function as a hierarchical identity-based encryption scheme (HIBE), which enables secure communication (e.g., via e-mails) inside the company. We call the mechanism *HIBE together with blind decryption protocol*, or HIBE-BDP for short. The mechanism uses as building block *blind* HIBE, which is a generalization of *blind* IBE [GH07]. A special case of our mechanism, IBE-BDP, solves the problem of blind decryption, which appeared in the literature, considering only one isolated retailer rather than a chain of them.

Keywords: blind HIBE, blind decryption, provable security, standard model.

1 Introduction

Motivation. Consider the following situation in trading encrypted information: over the Internet, a company owns a chain of retailers who sell digital information (e.g., music, magazine) using their websites. The information is available in encrypted form, namely ciphertexts, on the websites. A buyer, after browsing the summaries, must pay some money to have its choice of ciphertexts decrypted by the corresponding retailers. The problem is: the buyer wishes to hide its choice of purchases, namely he/she wants to have his/her choice of ciphertexts decrypted by the retailers in a blind manner; while the company and retailers want to make sure that the buyer cannot get more than what he/she pays (e.g., the buyer cannot obtain $v + 1$ plaintexts while only paying for v ones).

In this work, we propose a novel mechanism to solve the above problem. Additionally, it can function as a hierachical identity-based encryption scheme (HIBE), which enables secure communication (e.g., via e-mails) inside the company. We call the mechanism *HIBE together with blind decryption protocol*, or HIBE-BDP for short. Some highlighted functionalities of HIBE-BDP are as follows: (1) it supports everything a HIBE does. (2) Leaf identities[1], which represents the retailers, additionally support blind decryption protocols (with buyers). (3) Everyone, and in particular the root identity (the headquarters) and parent identities, can create ciphertexts the retailers will sell. This capability captures real situations in practice where sellers are not producers. (4) A current retailer, a leaf identity, can give up selling and freely set up new "child retailers". We expect this flexibility is extremely welcome in practice once a retailer is overloaded with what needs to sell.

HIBE-BDP uses as its building block *blind* HIBE, which is a generalization of *blind* IBE [GH07]. We consider syntax and define security notions for HIBE-BDP, and prove that our generic construction of HIBE-BDP from blind HIBE meet the notions if the building block blind HIBE is secure. Two concrete blind HIBE schemes, which are sufficient as building blocks for the construction of HIBE-BDP, are also proposed and analysed. These schemes are based on the HIBE schemes of Boneh-Boyen [BB04] and Chatterjee and Sakar [CS06], and can be seen as hierachical versions of the blind IBE schemes in [GH07].

Previous and related works. The problem of blind decryption has already appeared in [SY96], [MSO96], [SJ00]. These works considered only one retailer as a company itself. To our knowledge, no work in the literature has considered the problem when it comes to a chain of retailers instead of one, let alone combining HIBE with BDP. Other seemingly related concepts are private information retrieval (PIR) and oblivious transfer (OT). There is a huge literature on PIR and OT. We however note that the situation in trading encrypted information is apparently not the research motivation on PIR and OT. As a result, syntax and security notions of PIR and OT are different from those of BDP and HIBE-BDP considered in this work. Another point is that PIR and OT only consider two players, i.e., one receiver (user) and one sender (database), which totally differs from HIBE-BDP.

* Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku Tokyo, 152-8550, Japan (ltphong@crypt.ss.titech.ac.jp)

[1] Here and hereafter, we use the term leaf identities to indicate identities who are not a parent identity of any one.

Our Contributions. In short, the contributions of this work are: (1) considering blind HIBE and analyzing concrete blind HIBE schemes, which are generalizations of Green and Hohenberger [GH07], and (2) providing definition for HIBE-BDP together with its security notions, and proposing a generic construction of HIBE-BDP based on any secure blind HIBE scheme. We consider the latter as the main contribution of this paper.

2 Technical Preliminaries

We will use essentially the same presentation and wording as [GH07] in this section and Section 3. Let $\mathsf{BMsetup}$ be an algorithm that, on input a security parameter κ, outputs the parameters for a bilinear mapping as $\gamma = (q, g, G, G_T, e)$, where g generates G, $e : G \times G \rightarrow G_T$, and q is the order of G and G_T. We will need the following complexity assumption made in these groups.

Decisional Bilinear Diffie-Hellman (DBDH) Assumption [BF01]. Let $\mathsf{BMsetup}(\kappa) \rightarrow (q, g, G, G_T, e)$. For all p.p.t. adversaries $\mathcal{A}$, the value $|\Pr[b' = b] - 1/2|$ is negligible in the following experiment: $a, b, c, d \stackrel{\$}{\leftarrow} Z_q$; $x_0 \leftarrow e(g,g)^{abc}$; $x_1 \leftarrow e(g,g)^d$; $b \stackrel{\$}{\leftarrow} \{0,1\}$; $b' \leftarrow \mathcal{A}(g, g^a, g^b, g^c, x_b)$.

Known Discrete-Logarithm-Based, Zero Knowledge Proofs. We use known techniques for proving statements about discrete logarithms, such as (1) proof of knowledge of a discrete logarithm modulo a prime [Sch91], (2) proof that a committed value lies in a given integer interval [CFT98, CM99, Bou00], and also (3) proof of conjunction of any of the previous [CDS94]. These protocols are secure under the discrete logarithm assumption, although some implementation of (2) requires the Strong RSA assumption [BP97, F097]. When referring to the proofs above, we use the notation of Camenisch and Stadler [CS97]. For instance, $PoK\{(x, r): y = g^x h^r \wedge 1 \leq x \leq n\}$ denotes a zero-knowledge proof of knowledge of integers x and r such that $y = g^x h^r$ and $1 \leq x \leq n$. All values not enclosed in ()'s are assumed to be known to the verifier.

3 HIBE and blind HIBE

3.1 Definitions

Hierachical Identity-based Encryption Scheme (HIBE) [GS02, HL02]. A HIBE consists of four algorithms: Setup, $\mathsf{Extract}$, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$. In a HIBE, identities are vectors. A vector of dimension j represents an identity at depth j, denoted as $ID_{|j} = (I_1, \ldots, I_j)$ where the components $I_1, \ldots, I_j \in \mathcal{I}$ for some set $\mathcal{I}$. The detailed description and functionality of the algorithms are as follows:

– In the $\mathsf{Setup}(\kappa, l) \rightarrow (params, msk)$ algorithm, on input a security parameter κ and the maximum depth l of the HIBE, the master authority outputs master parameters and a master secret key $(params, msk)$.

– In the $\mathsf{Extract}(\mathcal{P}_{ID|j-1}(sk_{ID|j-1}), \mathcal{U}\ (ID_{|j}=(I_1, \ldots, I_j))) \rightarrow (ID_{|j}, sk_{ID|j})$ protocol, an honest user $\mathcal{U}$ with identity $ID_{|j} = (I_1, \ldots, I_j)$ obtains the corresponding secret key $sk_{ID|j}$ from the parent identity $ID_{|j-1} = (I_1, \ldots, I_{j-1})$ or outputs an error message. The parent identity output is **the identity** $ID_{|j}$ or an error message.

– In the $\mathsf{Encrypt}(params, ID_{|j}, m) \rightarrow C$ algorithm, on input identity $ID_{|j} \in \mathcal{I}^j$ and a message $m \in \mathcal{M}$, any party can output a ciphertext C.

– In the $\mathsf{Decrypt}(sk_{ID|j}, C) \rightarrow m$, on input a ciphertext C, the user with $sk_{ID|j}$ can output a message $m \in \mathcal{M}$ or an error message.

Definition 1 (IND-sID-CPA security for HIBE scheme [CHK04]). *Let κ, l be the security parameter and maximum depth of HIBE, and $\mathcal{M}$ the message space. The HIBE is IND-sID-CPA-secure if every p.p.t. adversary $\mathcal{A}$ has an advantage negligible in κ, l for the following game with a challenger: (1) $\mathcal{A}$ outputs a target identity ID^*. (2) The challenger runs $\mathsf{Setup}(\kappa, l)$ to obtain $(params, msk)$ and gives params to $\mathcal{A}$. (3) $\mathcal{A}$ may make polynomially-many key extraction queries ID. In response, the challenger runs the $\mathsf{Extract}$ algorithm on input ID to obtain the corresponding private key sk_{ID} and gives it to $\mathcal{A}$. The only restrictions are: ID is not ID^* and is not a prefix of ID^*. (4) $\mathcal{A}$ outputs two equal-length messages m_0, m_1. The challenger chooses a random bit b, and gives $\mathcal{A}$ the challenge ciphertext $C^* \leftarrow \mathsf{Encrypt}(params, ID^*, m_b)$. (5) $\mathcal{A}$ may continue to make key extraction queries under the same conditions as before. (6) $\mathcal{A}$ outputs $b' \in \{0,1\}$. The advantage of $\mathcal{A}$ in the game is defined as $|\Pr[b' = b] - 1/2|$.*

On IND-ID-CPA security for HIBE. This notion of security is stronger than the above notion, allowing the adversary to choose a target identity at Step 4 in the above game. We however note that the weak IND-sID-CPA security is enough for our construction of HIBE-BDP.

Blind HIBE. A blind HIBE scheme consists the same algorithms Setup, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$ as in a traditional HIBE one, but the protocol $\mathsf{Extract}$ is replaced by a new protocol $\mathsf{BlindExtract}$:

– In the $\mathsf{BlindExtract}(\mathcal{P}_{ID|j-1}(sk_{ID|j-1}), \mathcal{U}(ID_{|j} = (I_1, \ldots, I_j))) \rightarrow (nothing, sk_{ID|j})$ protocol, an honest user $\mathcal{U}$ with identity $ID_{|j} = (I_1, \ldots, I_j)$ obtains the corresponding secret key $sk_{ID|j}$ from the parent identity $ID_{|j-1} = (I_1, \ldots, I_{j-1})$ or outputs an error message. The parent identity output is **nothing** or an error message.

We now define security for blind HIBE, which is informally any IND-sID-CPA HIBE scheme with a $\mathsf{BlindExtract}$ protocol satisfying two below properties:

1. Leak-free Extract [GH07]: a potentially malicious user cannot learn anything by executing the $\mathsf{BlindExtract}$ protocol with a parent identity which she

could not have learned by executing the Extract protocol with the parent identity; moreover, as in Extract the user must know the identity for which she is extracting the key.

2. Selective-failure Blindness [CNS07]: a potentially malicious parent identity cannot learn anything about the user's choice of identity during the BlindExtract protocol (more than what it has already known before BlindExtract); moreover, the parent identity cannot cause the BlindExtract protocol to fail in a manner dependent on the user's choice of identity.

Definition 2 (Leak-Free Extract [GH07])**.** *A protocol BlindExtract$(\mathcal{P},\mathcal{U})$ associated with an HIBE scheme* Π*=(Setup, Extract, Encrypt, Decrypt) is leak-free if for all efficient adversaries $\mathcal{A}$, there exists an efficient simulator $\mathcal{S}$ such that for every value κ and l, no efficient distinguisher $\mathcal{D}$ can distinguish whether $\mathcal{A}$ is playing with Game Real or Game Ideal with non-negligible advantage:*

Game Real: *Run $(params, msk) \leftarrow$ Setup(κ, l). As many time as $\mathcal{D}$ wants, $\mathcal{A}$ chooses an identity $ID_{|j} = (I_1, \ldots, I_j)$ and executes the BlindExtract protocol with $\mathcal{P}_{ID|j-1}$:*

$$\mathsf{BlindExtract}(\mathcal{P}_{ID|j-1}(sk_{ID|j-1}), \mathcal{A}(ID_{|j})).$$

Game Ideal: *Run $(params, msk) \leftarrow$ Setup(κ, l). As many time as $\mathcal{D}$ wants, $\mathcal{S}$ chooses an identity $ID_{|j} = (I_1, \ldots, I_j)$ and queries the trusted party $\mathcal{P}_{ID|j-1}$ to obtain its output in*

$$\mathsf{Extract}(\mathcal{P}_{ID|j-1}(sk_{ID|j-1}), \mathcal{S}(ID_{|j})).$$

Here, $\mathcal{D}$ and $\mathcal{A}$ (or $\mathcal{S}$) may communicate at any time.

A nice property of the above definition is that any key extraction protocol with leak-freeness (regardless of whether blindness holds or not) composes into the existing security definitions for HIBE, which is formally stated in the following lemma, which is an obvious generalization of its IBE-based counterpart in [GH07].

Lemma 3. *If* Π *=(Setup, Extract, Encrypt, Decrypt) is an IND-sID-CPA-secure (resp., IND-ID-CPA) HIBE scheme and BlindExtract associated with* Π *is a leak-free protocol, then* Π' *=(Setup, BlindExtract, Encrypt, Decrypt) is an IND-sID-CPA-secure (resp., IND-ID-CPA) HIBE scheme.*

We proceed to formally define the second property of *selective-failure blindness*.

Definition 4 (Blindness of Blind HIBE [CNS07])**.** *A protocol $P(\mathcal{A}_{ID|j-1}(\cdot), \mathcal{U}(\cdot,\cdot))$ is said to be selective-failure blind if every p.p.t. adversary $\mathcal{A}_{ID|j-1}$ has a negligible advantage in the following game: First of all, (params, msk) $\leftarrow$ Setup(κ, l). The master key msk is used to generate the private key $sk_{ID|j-1}$ for $\mathcal{A}_{ID|j-1}$ while params is given to $\mathcal{U}$. $\mathcal{A}_{ID|j-1}$ first outputs two values $I_0, I_1 \in \mathcal{I}$. A random $b \in \{0,1\}$ is chosen and let $ID_{b|j} = (ID_{|j-1}, I_b)$. $\mathcal{A}_{ID|j-1}$ is given a black-box access to two oracles $\mathcal{U}(params, ID_{b|j})$ and $\mathcal{U}(params, ID_{b-1|j})$. The $\mathcal{U}$ algorithms produce local outputs sk_b and sk_{b-1} respectively. If $sk_b \neq \perp$ and $sk_{b-1} \neq \perp$, then $\mathcal{A}_{ID|j-1}$ is given (sk_0, sk_1). If $sk_b = \perp$ and $sk_{b-1} \neq \perp$, then $\mathcal{A}_{ID|j-1}$ is given $(\perp, \epsilon)$. If $sk_b \neq \perp$ and $sk_{b-1} = \perp$, then $\mathcal{A}_{ID|j-1}$ is given $(\epsilon, \perp)$. If $sk_b = \perp$ and $sk_{b-1} = \perp$, then $\mathcal{A}_{ID|j-1}$ is given $(\perp, \perp)$. Finally, $\mathcal{A}_{ID|j-1}$ outputs its guess b'. We define the advantage of $\mathcal{A}_{ID|j-1}$ in this game as $|\Pr[b' = b] - 1/2|$.*

We finally arrive at the following definition.

Definition 5 (Secure Blind HIBE)**.** *A blind HIBE* Π *= (Setup, BlindExtract, Encrypt, Decrypt) is IND-sID-CPA-secure if and only if: (1) its corresponding HIBE is IND-sID-CPA secure, and (2) BlindExtract is leak-free and selective-failure blind.*

3.2 HIBE Schemes with Efficient BlindExtract Protocols

In this section, we build efficient BlindExtract protocols for: (1) the IND-sID-CPA-secure HIBE due to Boneh and Boyen [BB04] and (2) the IND-ID-CPA-secure HIBE proposed by Chatterjee and Sakar [CS06]. The protocols are HIBE versions of their counterparts in [GH07]. Since these schemes share a similar structure, we begin by describing their common parts.

– Setup(κ, l): Let $\gamma = (q, g, G, G_T, e)$ be the output of BMsetup(κ). Choose $\alpha \xleftarrow{\$} Z_q$, and set $g_1 \leftarrow g^\alpha$. Choose $g_2, h_1, \ldots, h_l \xleftarrow{\$} G$. Select functions $F_k : \mathcal{I} \rightarrow G$ for $1 \leq k \leq l$. (The descriptions of F_k will be defined specific to the schemes below.) Output $params = (\gamma, g_1, g_2, h_1, \ldots, h_l, F_k)$ and $msk = g_2^\alpha$.

– Extract$(\mathcal{P}_{j-1}(sk_{ID|j-1}), \mathcal{U}(ID_{|j} = (I_1, \ldots, I_j))) \rightarrow (ID, sk_{ID|j})$: The private key of identity $ID_{|j}$ is of the form $sk_{ID|j} = (g_2^\alpha \Pi_{k=1}^j F_k(I_k)^{r_k}, g^{r_1}, \ldots, g^{r_j})$. Such a private key can be generated by $\mathcal{P}_{j-1}$ as follows: let $sk_{ID|j-1} = (d_0, \ldots, d_{j-1})$. $\mathcal{P}_{j-1}$ picks random $r_j \xleftarrow{\$} Z_q$ and sets $sk_{ID|j} = (d_0 F_j(I_j)^{r_j}, d_1, \ldots, d_{j-1}, g^{r_j})$.

– Encrypt$(params, ID = (I_1, \ldots, I_j), m) \rightarrow C$: $t \xleftarrow{\$} Z_q$, $C \leftarrow (C_0 = m \times e(g_1, g_2)^t, C_1 = g^t, B_1 = F_1(I_1)^t, \ldots, B_j = F_j(I_j)^t)$.

– Decrypt$(sk_{ID|j}, C) \rightarrow m$: Consider an identity $ID = (I_1, \ldots, I_j)$. To decrypt a given ciphertext $C =(C_0, C_1, B_1, \ldots, B_j)$ using the private key $sk_{ID|j} = (d_0, \ldots, d_j)$, output

$$C_0 \frac{\Pi_{k=1}^j e(B_k, d_k)}{e(d_0, C_1)}$$

We proceed to describe the precise format of the private keys and corresponding BlindExtract protocols for particular HIBEs.

3.2.1 A BlindExtract Protocol for Boneh-Boyen HIBE

In the Boneh-Boyen HIBE [BB04], $\mathcal{I} = Z_q$ and the function $F_k : \mathcal{I} \rightarrow G$ is defined as $F_k(I) = h_k \cdot g_1^I$ for

$I \in \mathcal{I}$ and $1 \le k \le l$. The private key for identity $ID_{|j}$ is

$$sk_{ID|j} = (g_2^{\alpha} \cdot \Pi_{k=1}^{j}(h_k \cdot g_1^{I_k})^{r_k}, g^{r_1}, \ldots, g^{r_j}).$$

The protocol BlindExtract for this HIBE is described as follows. The players and their inputs are $\mathcal{P}_{j-1}(sk_{ID|j-1} = (d_0, \ldots, d_{j-1}))$ and $\mathcal{U}(ID = (I_1, \ldots, I_j))$. $\mathcal{U}$ first does the following: (1) chooses $y \xleftarrow{\$} Z_q$, (2) computes $h' \leftarrow g^y g_1^{I_j}$ and sends h' to $\mathcal{P}_{j-1}$, (3) executes $PoK\{(y, I_j)\colon h' = g^y g_1^{I_j}\}$ with $\mathcal{P}_{j-1}$. $\mathcal{P}_{j-1}$ in turn does the following steps: (4) if the proof fails to verify, abort, (5) chooses $r_j \xleftarrow{\$} Z_q$, (6) computes $d_0' \leftarrow d_0(h'h_j)^{r_j}$ and $d_j' \leftarrow g^{r_j}$, (7) sends $(d_0', d_1, \ldots, d_{j-1}, d_j')$ to $\mathcal{U}$. $\mathcal{U}$ finally does the following: (8) checks $e(d_0', g) = e(g_2, g_1)\, e(h'h_j, d_j')\, \Pi_{k=1}^{j-1} e(F_k(I_k), d_k)$ and chooses $z \xleftarrow{\$} Z_q$ if the check passes, (9) outputs $sk_{ID|j} \leftarrow (d_0'\ (d_j')^{-y}\ F_j(I_j)^z, d_1, \ldots, d_{j-1}, d_j' g^z)$.

Let Π_1 be the blind HIBE that combines the algorithms Setup, Encrypt, Decrypt and the protocol BlindExtract as above. We have the following theorem.

Theorem 6. *The protocol BlindExtract above is both leak-free and selective-failure blind. As a result, the blind HIBE Π_1 is IND-sID-CPA-secure (according to Definition 5) under the DBDH assumption.*

The proof of this theorem, which is similar to its IBE counterpart in [GH07] will be given in the full version of this paper.

3.2.2 A BlindExtract Protocol for Chatterjee-Sakar HIBE

In the HIBE scheme proposed by Chatterjee and Sakar [CS06], the set $\mathcal{I}$ is the set of bit strings of length N, where $N(= n \cdot m)$ is polynomial in κ, represented by n blocks of m bits. Define the function $F_k(I) = h_k \cdot \Pi_{i=1}^{n} u_i^{I[i]}$ for $1 \le k \le l$, where $I[1], \ldots, I[n]$ are m-bit segments of $I \in \mathcal{I}$, and $u_1, \ldots, u_n \in G$ are randomly chosen by the master authority in Setup algorithm. The private key for identity $ID_{|j}$ is

$$sk_{ID|j} = (g_2^{\alpha} \cdot \Pi_{k=1}^{j}(h_k \cdot \Pi_{i=1}^{n} u_i^{I_k[i]})^{r_k}, g^{r_1}, \ldots, g^{r_j}).$$

The protocol BlindExtract is almost the same as that of the previous section, except the following alterations. Parse I_j as $I_j = I_j[1] \cdots I_j[n]$. In (2), compute $h' \leftarrow g^y \Pi_{i=1}^{n} u_i^{I_j[i]}$. In (3), execute $PoK\{(y, I_j = I_j[1] \ldots I_j[n])\colon h' = g^y \Pi_{i=1}^{n} u_i^{I_j[i]} \wedge 0 \le I_j[i] < 2^m \forall 1 \le i \le n\}$. Follows the rest of the protocol as it is.

Let Π_2 the blind HIBE that combines Setup, Encrypt, Decrypt with the BlindExtract protocol.

Theorem 7. *The protocol BlindExtract in this section is both leak-free and selective-failure blind. As a result, the blind HIBE Π_2 is IND-ID-CPA-secure (according to Definition 5) under the DBDH assumption.*

The proof of this theorem, which is similar to its IBE counterpart in [GH07] will be given in the full version of this paper.

4 HIBE together with blind decryption protocol: HIBE-BDP

4.1 Syntax and Security Definitions

Syntax. Let Π = (Setup, Extract, Encrypt, Decrypt) be a HIBE scheme. A HIBE-BDP, denoted as Π_{bdp} = (Π, Enc, BlindDec), reuses the four algorithms of Π, and contains two additional algorithms: Enc and BlindDec. The algorithms Extract, Encrypt, Decrypt support all identities as in the HIBE, while the protocol BlindDec supports only leaf identities of the HIBE. The algorithm Enc requires as one of its input a leaf identity, although it can be used by any party. Denote Leaves the set of leaf identities, which depends on the (current) structure of the HIBE. The description and functionality of the two new algorithms are as follows:

– $\mathsf{Enc}(params, ID \in \mathsf{Leaves}, m) \rightarrow C$: On inputs $params$, a leaf identity ID, and a message m, Enc produces a ciphertext C. The purpose of this algorithm is to create ciphertexts which the retailers (leaf identities) will sell. We note that not only the retailers but also any party can use this algorithm. This captures real situations in practice where the owner's of the retailers (i.e., the company or the parent identities) themselves creates the ciphertexts (and send them to the retailers).

– $\mathsf{BlindDec}(\mathcal{P}_{ID}(sk_{ID}), \mathcal{U}(C)) \rightarrow (nothing, m)$: Every time an honest buyer $\mathcal{U}$ wants to buy the content inside a ciphertext C which is available from $\mathcal{P}_{ID}$ where $ID \in$ Leaves, she engages $\mathcal{P}_{ID}$ in a BlindDec protocol. At the end, $\mathcal{U}$ receives the content m while $\mathcal{P}_{ID}$ knows *nothing* about the choice of the ciphertext.

We proceed to define security notions for HIBE-BDP. There are three issues to be considered: HIBE-security, the privacy of buyer, and the security of retailers.

1. HIBE security and blindness. A HIBE-BDP must be secure as a HIBE, namely IND-sID-CPA-secure or IND-ID-CPA-secure. This will be easy since we will use secure HIBEs. Blindness of HIBE-BDP ensures the privacy of the buyer. Namely, the retailers cannot know more about the buyer's choice of ciphertexts after the BlindDec protocol than what it has already known before the BlindDec protocol. We will not formalize this intuition about blindness here, since the blindness of our construction of HIBE-BDP comes directly and obviously from the blindness of the underlying blind HIBE. We believe that doing so makes our presentation clearer.

2. Indistinguishability One-More (IND-OM) security. IND-OM security intuitively ensures that it is impossible for a (potentially malicious) buyer to get more than what he/she paid. We will use the one-more security approach, and yet in an indistinguishability style. This notion itself is new to this paper. Let us first present some intuitions behind the notion, and then move to the precise description. Recall that a malicious user, an adversary, can collect ciphertexts available from the websites of the retailers. We capture this ability by providing the adversary an encryption algorithm, in a left-or-right style. The adversary can

also engage the retailers in BlindDec protocols, so that BlindDec oracles are given. Note that the adversary can buy at the same time many pieces of information, so that concurrent BlindDec protocols are needed. This is also included in the security model. At the end, the adversary wins if after v times of querying the BlindDec oracles, it knows one-more bit used in the left-or-right encryption oracles; namely, it knows non-negligible information about the content of some ciphertext for which it did not pay. Conversely, a HIBE-BDP is ind-om-secure if no p.p.t. adversary can win. Note that ind-om security also implies that the adversary cannot decrypt a $(v+1)$-th ciphertext after v times of accessing to the BlindDec oracles. In other words, ind-om implies one-way one-more (OW-OM). The formal definition is as follows.

Definition 8 (IND-OM security for HIBE-BDP)**.** *Let Π_{bdp} = (*Π*, Enc, BlindDec) be a HIBE-BDP, where Π = (Setup, Extract, Encrypt, Decrypt). Consider the following game between a challenger and an adversary $\mathcal{A}$.*

Setup: *The challenger first runs Setup(κ) to obtain params and msk, and gives params to $\mathcal{A}$.*
Denote Leaves $=\{ID_1, \ldots, ID_k\}$ $(k \geq 1)$ the set of leaf identities of the HIBE.

Queries: *the adversary is allowed to make the following types of queries:*
– Encryption query $(ID_j \in \mathsf{Leaves}, m_0^{(i)}, m_1^{(i)})$: the challenger chooses a random bit, denoted as $b_{(j,i)} \stackrel{\$}{\leftarrow} \{0,1\}$, computes $C_{(j,i)} \leftarrow \mathsf{Enc}(params, ID_j, m_{b_{(j,i)}}^{(i)})$, and then returns $C_{(j,i)}$ to $\mathcal{A}$. The adversary is permitted to make u_j encryption queries to ID_j, thus $1 \leq i \leq u_j$.
– Blind decryption query $(ID \in \mathsf{Leaves}, C)$: the adversary $\mathcal{A}$ engages $\mathcal{P}_{ID}(sk_{ID})$ in a BlindDec$(\mathcal{P}_{ID}(sk_{ID}), \mathcal{A}(C))$ protocol. $\mathcal{A}$ can engages many BlindDec protocols with many different leaf nodes at the same time. The adversary is permitted to make v $(< u_1 + \cdots + u_k)$ blind decryption queries.

Output: *$\mathcal{A}$ outputs $v+1$ bits $b'_1, \ldots, b'_{v+1}$ and an injective map $\pi : \{1, \ldots, v+1\} \to \{1, \ldots, k\} \times \{1, \ldots, u\}$, where $u = \max\{u_1, \ldots, u_k\}$. Denote the above adversary as $\mathcal{A}(u_1, \ldots, u_k, v)$.*

We say that $\mathcal{A}$ wins if b'_i is the right guess of $b_{\pi(i)}$ for all $1 \leq i \leq v+1$. Define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}^{ind-om}_{\mathsf{HIBE\text{-}BDP}}(\mathcal{A}) = \Pr[b'_i = b_{\pi(i)} \forall 1 \leq i \leq v+1] - \frac{1}{2}.$$

If the advantage is either negligle or negative for all p.p.t. adversaries $\mathcal{A}$, we say that the HIBE-BDP is ind-om-secure.

Remarks and Discussions about IND-OM. Firstly, we emphasize that, unusually, the absolute value cannot be taken when defining the above advantage function, and one has to consider adversaries with *negative* advantage. In fact, if the absolute value is taken, then an adversary doing nothing, just returning random bits has advantage $|1/2^{v+1} - 1/2|$, which is not negligible at all.

Secondly, consider again the situation between the retailers and the buyer as in Section 1. We note that, in practice, some summaries and/or keywords of the contents inside the ciphertexts should also be available on the websites so that the buyer can make choices. The IND-OM security ensures that even so, the adversary still has negligible knowledge about the other parts of the contents. Our IND-OM notion is stronger than the one-more decryption security considered in [SJ00]. In fact, our notion allows the adversary to adaptively encrypt messages of its own choice, while that of [SJ00] does not. All messages in the notion of [SJ00] are randomly chosen, and the corresponding ciphertexts are non-adaptively given to the adversary at the beginning.

4.2 The construction of HIBE-BDP

In this section, we show how to turn any HIBE supporting blind key extract (namely, Blind HIBE), into a HIBE-BDP. Let Π = (Setup, Extract, Encrypt, Decrypt) be a HIBE and Π' = (Setup, BlindExtract, Encrypt, Decrypt) its corresponding blind HIBE. To build the HIBE-BDP Π_{bdp} = (Π, Enc, BlindDec), we just have to construct the Enc algorithm and the BlindDec protocol. The construction is as follows.

The Construction of Π_{bdp}

–Enc($params$, $ID \in$ Leaves,m): $I \stackrel{\$}{\leftarrow} \mathcal{I}$, $ID' \leftarrow (ID, I)$, $\hat{C} \stackrel{\$}{\leftarrow}$ Encrypt($params$, ID', m). Output $C \leftarrow (ID', \hat{C})$.
–BlindDec($\mathcal{P}_{ID}(sk_{ID})$,$\mathcal{U}(C)$): $\mathcal{U}$ first parses C as $(ID', \hat{C})$. $\mathcal{U}$ then runs (with $\mathcal{P}_{ID}$) the protocol BlindExtract$(\mathcal{P}_{ID}(sk_{ID}), \mathcal{U}(ID')) \rightarrow (nothing, sk_{ID'})$. $\mathcal{U}$ finally outputs Decrypt$(sk_{ID'}, \hat{C})$.

This construction of HIBE-BDP, which is quite simple, and can be seen as a mixture between the HIBE scheme Π and its blind version Π'. The HIBE scheme Π is kept the same, while the BlindExtract protocol of Π' is utilised only by leaf identities via BlindDec. One can imagine a leaf identity (a retailer) as a "parent identity" of its ciphertexts, and a user bought a ciphertext (namely, a private key in this context) becomes a "child identity" of the leaf identity.

We proceed to consider the security of the above construction. The private keys a user can get is below the leaf identities, so these keys cannot affect the security of the HIBE, and hence the HIBE part of Π_{bdp} retains security. Furthermore, a user only engages a retailer in BlindExtract protocols, so that blindness of Π_{bdp} is obvious from the blindness property of BlindExtract. We formally state these facts in the following theorem.

Theorem 9. *The following statements holds true:*
(1) Π_{bdp} satisfies blindness.
(2) The HIBE part Π retains security as it is.

We now move to the ind-om security, which is ensured by the following theorem.

Theorem 10. *Let $\mathcal{A}(u_1, \ldots, u_k, v)$ be an ind-om adversary against the HIBE-BDP Π_{bdp}. Then there exist a distinguisher $\mathcal{A}_1$ (against the leak-freeness of Π') and*

an adversary $\mathcal{A}_2$ (against the IND-sID-CPA security of Π), whose resources are essentially the same as that of $\mathcal{A}$ such that

$$\mathbf{Adv}^{ind-om}_{\Pi_{bdp}}(\mathcal{A}) \leq \mathbf{Adv}^{leak-free}_{\Pi'}(\mathcal{A}_1) + ku\mathbf{Adv}^{ind-sid-cpa}_{\Pi}(\mathcal{A}_2),$$

where $u = \max\{u_1, \ldots, u_k\}$.

The intuition behind its proof is as follows: the coalition of some child identities cannot affect other child identities. The proof of this theorem will be given in the full version of this paper.

5 Conclusion

We have considered blind HIBE schemes and used them to construct HIBE-BDP. The schemes would be useful in trading encrypted information: its HIBE part supports secure communication inside the company, while its BDP part ensures security for both retailers and buyers. We furthermore expect other applications of HIBE-BDP as well as blind HIBE in the future.

References

[Bou00] F. Boudot. Efficient Proofs that a Committed Number Lies in an Interval. EUROCRYPT 2000, 431–444, 2000.

[BB04] D. Boneh and X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In Advances in Cryptology (EUROCRYPT 2004), Springer LNCS 3027, 223–238, 2004.

[BF01] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In J. Kilian, editor, Proceedings of Crypto 2001, volume 2139 of LNCS, 213–229. Springer-Verlag, 2001.

[BP97] N. Baric and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In EUROCRYPT '97, vol. 1233 of Lecture Notes in Computer Science, 480–494. Springer–Verlag, 1997.

[CDS94] R. Cramer, I. Damgard, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Y. G. Desmedt, editor, Advances in Cryptology — CRYPTO '94, volume 839 of Lecture Notes in Computer Science, 174–187. Springer Verlag, 1994.

[CFT98] A. Chan, Y. Frankel, and Y. Tsiounis. Easy come – easy go divisible cash. In K. Nyberg, editor, Advances in Cryptology — EUROCRYPT '98, volume 1403 of Lecture Notes in Computer Science, 561–575. Springer Verlag, 1998.

[CNS07] Jan Camenisch, Gregory Neven, and abhi shelat. In M. Naor, editor, Advances in Cryptology - EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, 573–590 Springer-Verlag, 2007.

[CM99] J. Camenisch and M. Michels. Proving in Zero-Knowledge That a Number Is the Product of Two Safe Primes. In Eurocrypt '99, LNCS 1592, 107–122 Springer-Verlag, 1999.

[CHK03] R. Canetti, S. Halevi, and J. Katz. A Forward-Secure Public-Key Encryption Scheme. Eurocrypt 2003, LNCS vol. 2656, Springer-Verlag, 255–271, 2003.

[CHK04] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In Advances in Cryptology—EUROCRYPT '04, volume 3027 of LNCS, 207–222. Springer-Verlag, 2004.

[CS97] J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups In Advances in Cryptology–CRYPTO '97, 410–424, 1997.

[CS06] S. Chatterjee and P. Sarkar. HIBE With Short Public Parameters Without Random Oracle. ASIACRYPT 2006, 145–160, 2006.

[F097] E. Fujisaki and T. Okamoto. Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations. CRYPTO 1997, 16–30, 1997.

[GH07] M. Green and S. Hohenberger. Blind Identity-Based Encryption and Simulatable Oblivious Transfer. ASIACRYPT 2007, 265–282. Available at http://eprint.iacr.org/2007/235.

[GS02] C. Gentry, A. Silverberg. Hierarchical ID-based cryptography, Advances in Cryptology – Asiacrypt'02, LNCS 2501, Springer-Verlag, 548–566, 2002.

[HL02] J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption. Advances in Cryptology – Eurocrypt 2002, LNCS vol. 2332, Springer-Verlag, 466–481, 2002.

[MSO96] M. Mambo, K. Sakurai, E. Okamoto. How to Utilize the Transformability of Digital Signatures for Solving the Oracle Problem. ASIACRYPT 1996, 322–333, 1996.

[Sch91] C. P. Schnorr. Efficient Signature Generation for Smart Cards. J. Cryptology 4(3), 161–174, 1991.

[SJ00] C. P. Schnorr and M. Jakobsson. Security of Signed ElGamal Encryption. In Asiacrypt 2000, LNCS 1976, 458–469, Springer-Verlag, 2000.

[SY96] K. Sakurai, and Y. Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. Proc. 1st Information Hiding Workshop, Cambridge, U.K. Springer LNCS 1174, 257–264, 1996.