Broadcast Encryption with Multiple Trust Centers and Dynamic Coalitions

Kent D. Boklan[1], Alexander W. Dent[2], and Christopher A. Seaman[3]

[1] Queens College, City University of New York, USA
[2] Royal Holloway, University of London, UK
[3] Graduate Center, City University of New York, USA

Abstract. In this paper we extend the notion of hierarchical identity-based encryption with wildcards (WIBE) from the domain of a single Trusted Authority (TA) to a setting with multiple, independent Trusted Authorities each with their own WIBE. In this multi-trust-authority WIBE environment, a group of TA's may form coalitions, enabling secure communication across domains. These coalitions may be temporary or dynamic in the sense that individual coalition TA members may be added or removed at any time. This allows the broadcast of confidential messages to large groups of users within a coalition with a single ciphertext. We provide a full syntax and security model for multi-trust-authority WIBEs, and give a constructions based on the Boneh-Boyen WIBE scheme for both passive and active attackers.

1 Introduction

Identity-based encryption (IBE) [?] is an attractive alternative to public-key encryption. Public-key encryption (PKE) allows for encryption only after obtaining a certified copy of the recipients public key. In identity-based encryption, a message is encrypted using a personal identifier such as an email address rather than using a certified public key obtained from a public-key infrastructure. The public key infrastructure is replaced by an identification system and a single public set of common parameters.

A hierarchical identity-based encryption (HIBE) [?] is an extension of identity-based encryption with identities organised in a tree with a single root master key. Thus, identities in a HIBE are a sequence of bitstrings, e.g. ("City University of New York", "Computer Science", "Bob Smith"). The identity hierarchy must mirror the trust hierarchy within an organisation as the private key for any identity can be used to generate a private key for any subordinate identity. One-to-many encryption may be achieved within a hierarchy by using a hierarchical identity-based encryption with wildcards (WIBE) [?]. In a WIBE scheme, encryption is performed with respect to a pattern of identities and wildcards. An identity is said to match the pattern if every non-wildcard level of the pattern is the same as the identity. A ciphertext can be decrypted by any user whose identity matches the pattern under which the message was encrypted.

We present an extension of the WIBE concept to a situation with multiple trusted authorities. Multiple-trust-authority WIBE (MTA-WIBE) schemes allow trust authorities to implement instances of the WIBE scheme (independent of any other trust authority). However, an MTA-WIBE allows trust authorities to form coalitions which enable secure cross-domain communications. These coalitions may be temporary or dynamic in the sense that individual coalition members may be added or removed at any time. The WIBE functionality allow encrypted messages to be sent to a large set of users within the coalition simultaneously. A ciphertext can only be decrypted by a user if (a) their trust authority is in the coalition, and (b) their user identity matches the pattern under which the ciphertext was encrypted. Coalition formation is achieved by a two-stage process in which trust authorities first exchange (public) messages and then broadcast (public) "update" messages to members of their hierarchy. This allows members to form *coalition decryption keys* which allow ciphertexts to be decrypted.

Other researchers have considered the question of developing IBE systems with multiple trusted authorities. For example, a scheme proposed by Paterson and Srinivasan [?] and another by Boklan *et al.* [?] introduced multiple-trust-authority IBE systems which allow trusted authorities to interact in order to derive a shared IBE system. The Paterson and Srinivasan [?] paper constructed an IBE scheme which supported multiple trust authorities in a way which makes it infeasible for an attacker to determine which trust authority's public parameters was used to form the ciphertext - i.e. the ciphertext preserves the anonymity of the trust authority. However, the Paterson and Srinivasan scheme does not allow trust authorities to form trust coalitions. The Boklan *et al.* scheme [?] allows trust authorities to cooperate to form trust coalitions, in the sense that within the coalition a private key issued by TA_i for an identity ID can be translated into a private key issued by TA_j for the same identity. However, in order to achieve this functionality, the scheme requires that the coalition trust authorities setup their master private keys simultaneously. Furthermore, every trust authority can deduce the master private key of every other trust authority. This is clearly a disadvantage in any setting where the trust authorities share anything less than complete trust in each other. Unlike our scheme, neither earlier scheme supports dynamic coalitions, hierarchical identity-based encryption, or one-to-many communication.

We provide a full syntax and security model for an MTA-WIBE scheme. We give a selective-identity instantiation based on the Boneh-Boyen WIBE scheme [?,?]. We also give generic methods to transform a selective-identity scheme into a fully secure scheme, and to transform a passively secure scheme into an actively secure scheme. This latter transform is a novel implementation of the Boneh-Katz transform [?] and is the most efficient generic transform for creating IND-CCA2 secure WIBEs or MTA-WIBEs from IND-CPA WIBEs or MTA-WIBEs in the literature.

Usage Scenarios We believe that MTA-WIBEs are useful in a variety of contexts. For example, suppose that a number of universities (e.g. "NYU", "CUNY", and "ENS") have independent MTA-WIBEs with a common naming convention (e.g. (SCHOOL, DEPARTMENT, INDIVIDUAL)). If these universities were to form a coalition, then a message encrypted using pattern (*,"Computer Science", *) could be decrypted by any member of the computer science department in any of the three universities in the coalition. Alternatively, a message encrypted using the pattern ("NYU", *, "Bob Smith") could only be decrypted by an individual named Bob Smith at NYU. We believe that MTA-WIBEs can be used for efficient communication across organisations (with common naming conventions) for shared projects.

Another usage scenario is within the realm of hardware distribution. Suppose a number of companies produce sensors for use in an ad-hoc network (including, e.g., "IBM") and suppose that these sensors can be classified according to the function they perform (including, e.g., "climate sensor"). We assume that there is a common naming structure for these sensors (e.g. (MANUFACTURER, SENSOR TYPE, PROJECT)). If the manufacturers agree to form a coalition, then a message encrypted using the coalition parameters and the pattern (*, "climate sensor", "Project Intercept") could be decrypted by any climate sensor on Project Intercept. Alternatively, a message encrypted using the pattern ("IBM", "climate sensor", *) can only be decrypted by IBM's climate sensors. This provides a method to address all sensors within a project (for project information distribution) or to address all sensors produced by an individual manufacturer (e.g. for software patching or update).

2 Multiple-trust-authority WIBEs

Throughout the paper we will use standard notation for algorithms and assignment – see Appendix A.1.

2.1 Syntax

A Trusted Authority is the root of a domain of trust with responsibilities over the namespace of its organization. In general we will refer to a Trusted Authority TA as a hierarchy of identities of the form $ID = (ID_0, ID_1, \ldots, ID_k)$ with the same first identity ($ID_0 = TA$) and maximum depth of L. Given a population of TA's $\mathcal{U} = \{TA_1, TA_2, \ldots, TA_n\}$ we define a coalition $\mathcal{C} = \{TA_a, TA_b, \ldots, TA_\ell\} \subseteq \mathcal{U}$. We also define a pattern to be a vector of identities and wildcards, i.e. $P = (P_1, \ldots, P_k)$ where $P_i \in \{0,1\}^* \cup \{*\}$ for $1 \leq i \leq k$. We say that an identity $ID = (ID_0, \ldots, ID_k)$ matches a pattern $P = (P_0, \ldots, P_{k'})$, written $ID \in_* P$, if $k \leq k'$ and $P_i \in \{ID_i, *\}$ for all $1 \leq i \leq k$. A multi-trust-authority WIBE (MTA-WIBE) consists of a number PPT algorithms. The following algorithms may be used by a TA:

- `Setup`: This algorithm produces public parameters to be used by all trust authorities. This is written $\mathit{param} \xleftarrow{\$} \texttt{Setup}(1^k)$. These public parameters are assumed to be an implicit input to all other algorithms.
- `CreateTA`: This algorithm creates the master public/private keys for a trust authority with a particular name ("TA_i"). The algorithm takes as input the proposed name for the trusted authority ("TA_i") and outputs a master key-pair (pk_i, sk_i), written $(pk_i, sk_i) \xleftarrow{\$} \texttt{CreateTA}(``TA_i")$.
- `CoalitionBroadcast`: Once a set of trust authorities agree to setup a coalition between them, each trust authority runs this algorithm to produce the information which allows the other trust authorities in the coalition to produce coalition keys for the members of their hierarchy. For some coalition $\mathcal{C} \subseteq \mathcal{U}$ containing TA_i, trust authority TA_i uses its secret key and the public keys of participating authorities to generate public parameters specific to each other authority. This is written as $W_i \xleftarrow{\$} \texttt{CoalitionBroadcast}(TA_i, sk_i, \mathcal{C}, PK)$, where $PK = \{pk_j : TA_j \in \mathcal{C}\}$ is the set of master public keys in the coalition and $W_i = \{w_{i,j} : TA_j \in \mathcal{C} \setminus TA_i\}$ is the set of key update elements. Each $w_{i,j}$ is sent from TA_i to TA_j.
- `CoalitionUpdate`: After every member TA_i of the coalition has provided a message $w_{i,j}$ to TA_j, trust authority TA_j uses this algorithm to combine those messages to allow creation of coalition-specific secret keys. It outputs a message v_j to be broadcast to every member of TA_j's hierarchy (who then run the `CoalitionExtract` algorithm). This is written $v_j \xleftarrow{\$} \texttt{CoalitionUpdate}(TA_j, sk_j, \mathcal{C}, \hat{W}_j)$ where $\hat{W}_j = \{w_{i,j} : TA_i \in \mathcal{C} \setminus TA_j\}$ is the set of coalition parameters received by TA_j.

We now describe the algorithms required by the individual users.

- `Extract`: This algorithm is used by an individual to generate private keys for their subordinates (entities on the level below them in the hierarchical structure). The keys generated are specific to the TA's WIBE, although they may later be adjusted for use in a coalition environment. For entity $ID = (ID_0, ID_1, \ldots, ID_k)$ extracting a private key for subordinate $ID^\dagger = (ID_0, ID_1, \ldots, ID_k, ID')$ the algorithm outputs $d_{ID^\dagger} \xleftarrow{\$} \texttt{Extract}(ID, d_{ID}, ID')$.
- `CoalitionExtract`: Users in a trust authority's hierarchy may use this algorithm to adapt their TA-specific WIBE private key for use within a coalition. To accomplish this their TA, TA_i, must provide an adjustment parameter v_i to be combined with the user's private key d_{ID}. A user generates its coalition key as $c_{ID} \leftarrow \texttt{CoalitionExtract}(d_{ID}, v_i)$.
- `Encrypt`: This algorithm can be used by an individual to encrypt a message m to any individual whose identity matches a pattern P in the coalition $\mathcal{C}$. This is computed as $C \xleftarrow{\$} \texttt{Encrypt}(\mathcal{C}, PK, P, m)$ where $PK = \{pk_i : TA_i \in \mathcal{C}\}$. We assume that $\mathcal{C} = \{P_0\}$ whenever $P_0 \neq *$.
- `Decrypt`: This algorithm can be used to decrypt a ciphertext C under a coalition key c_{ID} and outputs either a message m or the error symbol $\perp$. We write this operation as $\texttt{Decrypt}(ID, c_{ID}, C)$. If no coalition is currently defined, then $c_{ID} \leftarrow d_{ID}$.

It is, of course, possible to extend the MTA-WIBE syntax so that coalition update values v_j are produced after a protocol interaction between trust authorities in the coalition, but we use the simpler broadcast case as it is sufficient for our instantiation. We require that the scheme is correct in the obvious sense that decryption "undoes" encryption for correctly generated trust authorities and coalitions.

2.2 Security Model

We provide a security model for an MTA-WIBE. We begin by defining a selective-identity sID-IND-CPA model.This is a game played between a PPT attacker $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ and a hypothetical challenger: (1) the attacker runs $(\mathcal{C}^*, P^*, \omega) \xleftarrow{\$} \mathcal{A}_0(1^k)$ where $\mathcal{C}^*$ is the list of TA identifiers in the challenge coalition, P^* is the challenge pattern, and ω is state information; (2) the challenger generates $\mathit{param} \xleftarrow{\$} \texttt{Setup}(1^k)$ and $(pk_i, sk_i) \xleftarrow{\$} \texttt{CreateTA}(TA_i)$ for all $TA_i \in \mathcal{C}^*$; (3) the attacker outputs a bit $b' \xleftarrow{\$} \mathcal{A}_1(\mathit{param}, PK, \omega)$ where $PK \leftarrow \{pk_i : TA_i \in \mathcal{C}^*\}$. During $\mathcal{A}_1$'s execution, it may access the following oracles:

- $\texttt{CreateTA}(TA)$: The oracle computes $(pk, sk) \xleftarrow{\$} \texttt{CreateTA}(TA)$ and returns pk. This oracle can only be queried for values of TA that do not already have an associated public key. This TA is labelled "honest". (All TA's in $\mathcal{C}^*$ are also labelled "honest".)
- $\texttt{SubmitTA}(TA, pk)$: This oracle associates the identity TA with the public key pk. It is used to model rogue TAs. This oracle can only be queried for values of TA that do not already have an associated public key. This TA is labelled "corrupt".
- $\texttt{CoalitionBroadcast}(TA, \mathcal{C})$: This oracle computes the coalition key update set $W \xleftarrow{\$} \texttt{CoalitionBroadcast}(TA, sk, \mathcal{C}, PK$ where TA is "honest", sk is the private key associated with TA, $\mathcal{C}$ is a coalition containing TA, and PK is the set of public keys for trust authorities in $\mathcal{C}$. The oracle returns the set $W = \{w_j \,:\, TA_j \in \mathcal{C} \setminus TA\}$.
- $\texttt{CoalitionUpdate}(TA, \mathcal{C}, \hat{W})$: The oracle computes the adjustment parameter $v \xleftarrow{\$} \texttt{CoalitionUpdate}(TA, sk, \mathcal{C}, \hat{W})$ where TA is honest, sk is the private key associated with TA, $\mathcal{C}$ is a coalition containing TA, and $\hat{W} = \{w_j \,:\, TA_j \in \mathcal{C}\}$ is the set of key update messages that purport to be from TA_j. The oracle returns the value v. Note that we do not require that $\hat{W}$ corresponds to the elements returned by $\texttt{CoalitionBroadcast}$.
- $\texttt{Corrupt}(ID)$: The oracle returns d_{ID} for the identity ID. Note that if $ID = TA$ then this method returns the private key sk associated with the trust authority TA. This oracle can only be queried for situations where TA is "honest". If $ID = TA$ then TA is labelled "corrupt".
- $\texttt{Encrypt}(m_0, m_1)$: The oracle returns $C^* \xleftarrow{\$} \texttt{Encrypt}(\mathcal{C}^*, PK, P^*, m_b)$ where PK is the set of public keys associated with trust authorities $TA \in \mathcal{C}$. This oracle can only be queried once and only on values with $|m_0| = |m_1|$.

The attacker is forbidden from corrupting an identity $ID \in_* P^*$ under a trust authority $TA \in \mathcal{C}^*$. The attacker's advantage is defined to be

$$Adv^{\texttt{sID}}_{\mathcal{A}}(k) = |\Pr[b' = 1 \,|\, b = 1] - \Pr[b' = 1 \,|\, b = 0]| \,.$$

We define extended notions of security in the usual way. The IND-CPA notion of security is identical to the sID-IND-CPA notion of security except that there is no $\mathcal{A}_0$ algorithm. The algorithm $\mathcal{A}_1$ takes 1^k as input and the encryption oracle changes so that it works as follows:

- $\texttt{Encrypt}(\mathcal{C}^*, P^*, m_0, m_1)$: The oracle returns $C^* \xleftarrow{\$} \texttt{Encrypt}(\mathcal{C}^*, PK, P^*, m_b)$ where PK is the set of public keys associated with trust authorities $TA \in \mathcal{C}$. This oracle can only be queried once, only on values with $|m_0| = |m_1|$, and only on coalitions $\mathcal{C}$ where every $TA \in \mathcal{C}$ is honest.

The IND-CCA2 notion of security is identical to the IND-CPA notion of security except that $\mathcal{A}_1$ has access to a decryption oracle:

- $\texttt{Decrypt}(\mathcal{C}, ID, C)$: This oracle checks whether the coalition key c_{ID} has been defined for the coalition $\mathcal{C}$ (via a $\texttt{CoalitionUpdate}$ oracle query). If not, the oracle returns $\perp$. Otherwise, the oracle returns $\texttt{Decrypt}(ID, c_{ID}, C)$. This oracle can only be queried on identities for which the trust authority $TA = ID_0$ is honest.

The attacker is forbidden from submitting $(\mathcal{C}^*, ID, C^*)$ to the decryption oracle for any identity $ID \in_* P^*$.

We note that this model allows for "rogue TAs" whose parameters are generated maliciously, rather than by the `CreateTA` oracle, as there is no requirement that $\mathcal{C}$ contain TA identities generated by the `CreateTA` oracle *except* for the coalition submitted to the `Encrypt` oracle. The `SubmitTA` oracle allows the attacker to define a public key for a rogue TA although this public key is only used by the `CoalitionBroadcast` oracle. We also note that the inability to query an oracle to obtain the coalition key c_{ID} does not represent a weakness in the model (assuming that c_{ID} and d_{ID} are secured in a similar manner) as c_{ID} can always be formed from d_{ID} and the public value v.

```
Setup(1^k):
  $g_1, g_2, u_{i,j} \xleftarrow{\$} \mathbb{G}^*$ for $0 \le i \le L$, $j \in \{0,1\}$
  $param \leftarrow (g_1, g_2, u_{0,0}, \ldots, u_{L,1})$
  Return $param$

CreateTA($TA$):
  $\alpha \xleftarrow{\$} \mathbb{Z}_p$
  $pk \leftarrow g_1^{\alpha}$; $sk \leftarrow g_2^{\alpha}$
  Return $(pk, sk)$

CoalitionBroadcast($TA, sk, \mathcal{C}, PK$):
  For each $TA_j \in \mathcal{C}$:
    $r_j \xleftarrow{\$} \mathbb{Z}_p$
    $w_{j,0} \leftarrow g_2^{\alpha}(u_{0,0} \cdot u_{0,1}^{TA_j})^{r_j}$
    $w_{j,1} \leftarrow g_1^{r_j}$
    $w_j \leftarrow (w_{j,0}, w_{j,1})$
  $W \leftarrow \{w_j \ : \ TA_j \in \mathcal{C} \setminus \{TA\}\}$
  Return $W$

CoalitionUpdate($TA, sk, \mathcal{C}, \hat{W}$):
  Parse $\hat{W}$ as $\{w_j \ : \ TA_j \in \mathcal{C}\}$
  Parse $w_j$ as $(w_{j,0}, w_{j,1})$
  $v_0 \leftarrow \prod_{TA_j \in \mathcal{C} \setminus \{TA\}} w_{j,0}$
  $v_1 \leftarrow \prod_{TA_j \in \mathcal{C} \setminus \{TA\}} w_{j,1}$
  $v \leftarrow (v_0, v_1)$
  Return $v$

CoalitionExtract($d_{ID}, v$):
  Parse $v$ as $(v_0, v_1)$
  Parse $d_{ID}$ as $(h, a_0, \ldots, a_k)$
  $h' \leftarrow h \cdot v_0$
  $a_0' \leftarrow a_0 \cdot v_1$
  Return $c_{ID} \leftarrow (h', a_0', a_1, \ldots, a_k)$

Extract($ID, d_{ID}, ID'$):
  If $ID = \varepsilon$ then
    $r_0, r_1 \xleftarrow{\$} \mathbb{Z}_p$
    $h \leftarrow g_2^{\alpha}(u_{0,0} \cdot u_{0,1}^{ID_0})^{r_0}(u_{1,0} \cdot u_{1,1}^{ID_1})^{r_1}$
    $a_0 \leftarrow g_1^{r_0}$; $a_1 \leftarrow g_1^{r_1}$
    Return $(h, a_0, a_1)$
  Else
    Parse $d_{ID}$ as $(h, a_0, \ldots, a_k)$
    $r_{k+1} \xleftarrow{\$} \mathbb{Z}_p$
    $h' \leftarrow h(u_{k+1,0} u_{k+1,1}^{ID'})^{r_{k+1}}$
    $a_{k+1} \leftarrow g_1^{r_{k+1}}$
    Return $(h', a_0, \ldots, a_{k+1})$

Encrypt($\mathcal{C}, PK, P, m$):
  $t \xleftarrow{\$} \mathbb{Z}_p$
  $C_1 \leftarrow g_1^t$
  If $i \in W(P)$ then $C_{2,i} \leftarrow (u_{i,0}^t, u_{i,1}^t)$
  If $i \notin W(P)$ then $C_{2,i} \leftarrow (u_{i,0} \cdot u_{i,1}^{P_i})^t$
  $C_3 \leftarrow m \cdot e(\prod_{TA_j \in \mathcal{C}} pk_j, g_2)^t$
  Return $(C_1, C_{2,1}, \ldots, C_{2,\ell}, C_3)$

Decrypt($ID, c_{ID}, C$):
  Parse $c_{ID}$ as $(h, a_0, \ldots, a_\ell)$
  Parse $C$ as $(C_1, C_{2,1}, \ldots, C_{2,\ell}, C_3)$
  If $i \in W(P)$ then
    Parse $C_{2,i}$ as $(\tilde{u}_0, \tilde{u}_1)$
    $C'_{2,i} \leftarrow \tilde{u}_0 \cdot \tilde{u}_1^{ID_i}$
  If $i \notin W(P)$ then $C'_{2,i} \leftarrow C_{2,i}$
  $m' \xleftarrow{\$} C_3 \cdot \prod_{i=1}^{\ell} e(a_i, C'_{2,i}) / e(C_1, h)$
  Return $m'$
```

Fig. 1. The Boneh-Boyen MTA-WIBE. Recall that any identity ID has $ID_0 = TA$. The `Extract` algorithm differentiates between initial key extraction by the TA and hierarchical extraction by a user. The `Decrypt` algorithm assumes that the depth of the decryption key and the depth of the ciphertext are equal. If the depth of the decryption key is shorter than the depth of the ciphertext, then the user can extract a key of a correct length and use the decryption algorithm.

3 Boneh-Boyen MTA-WIBE

We present a selective-identity IND-CPA secure MTA-WIBE based on the Boneh-Boyen MTA-WIBE. The scheme is given in Figure 1. Our scheme makes use of two prime-order groups $(\mathbb{G}, \mathbb{G}_T)$ and an efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. We assume that the size of the prime p is determined by the security parameter k.

We prove this algorithm secure in the sID-IND-CPA security model. The intuition behind the proof is that any coalition of trust authorities can be viewed as an extended hierarchy with a "ghost" trust authority at the top level. Each actual trust authority is represented as a first-level identity under this ghost TA and, through communication with the other trust authorities in the coalition, is able to determine a private key for their first-level identity under the ghost TA. More specifically, if we consider a coalition $\mathcal{C} = \{TA_1, \ldots, TA_n\}$ in which each TA has a private key $sk_i = g_2^{\alpha_i}$, then the ghost TA will have a private key $g_2^{\sum \alpha_i}$. Upon forming the coalition, the trust authority TA_j receives the messages

$$w_{i,j,0} \leftarrow g_2^{\alpha_i}(u_{0,0} \cdot u_{0,1}^{TA_j})^{r_i} \qquad w_{i,j,1} \leftarrow g_1^{r_i}$$

from each $TA_i \in \mathcal{C} \setminus \{TA_j\}$. This allows TA_j to form the private key

$$h \leftarrow g_2^{\sum_i \alpha_i}(u_{0,0} \cdot u_{0,1}^{TA_j})^{\sum_{i \neq j} r_i} \qquad a_1 \leftarrow g_1^{\sum_{i \neq j} r_i}$$

which is precisely the key that would be obtained if the ghost TA were to distribute a private key to the identity TA_j. The security of the multi-TA scheme then essentially follows from the security of the single-TA WIBE scheme, although care must be taken to show that the broadcast messages $w_{i,j}$ and v_i do not leak information about the private keys to the attacker.

We prove this theorem in two steps. The first step removes the wildcards to form an sID-IND-CPA secure MTA-HIBE (i.e. a WIBE scheme which doesn't support wildcards).

Theorem 1. *Suppose that there exists a PPT attacker $\mathcal{A}$ against the sID-IND-CPA security of the multi-TA Boneh-Boyen WIBE with advantage $Adv_{\mathcal{A}}^{\texttt{WIBE}}(k)$. Then there exists a PPT attacker $\mathcal{B}$ against the sID-IND-CPA security of the multi-TA Boneh-Boyen HIBE with advantage $Adv_{\mathcal{B}}^{\texttt{HIBE}}(k) = Adv_{\mathcal{A}}^{\texttt{WIBE}}(k)$.*

Theorem 1 is proven using the projection technique of Abdalla *et al.* [**?**]. For completeness a proof is given in Appendix B. The more interesting step is to show that the HIBE is secure. This is shown relative to the DBDH assumption:

Definition 1. *Let $(\mathbb{G}, \mathbb{G}_T)$ be groups of cyclic groups of prime order $p(k)$ with a bilinear map e and let g be a generator of $\mathbb{G}$. Let D_k be the distribution $\boldsymbol{x} \leftarrow (g, g^a, g^b, g^c, e(g,g)^{abc})$ for $a, b, c \xleftarrow{\$} \mathbb{Z}_p$. Let R_k be the distribution $\boldsymbol{x} \leftarrow (g, g^a, g^b, g^c, Z)$ for $a, b, c \xleftarrow{\$} \mathbb{Z}_p$ and $Z \xleftarrow{\$} \mathbb{G}_T$. An algorithm $\mathcal{A}$ has advantage*

$$Adv_{\mathcal{A}}^{\texttt{DBDH}}(k) = |\Pr[\mathcal{A}(\boldsymbol{x}) = 1 \,|\, \boldsymbol{x} \xleftarrow{\$} D_k] - \Pr[\mathcal{A}(\boldsymbol{x}) = 1 \,|\, \boldsymbol{x} \xleftarrow{\$} R_k]| \,.$$

The DBDH assumption holds if every PPT attacker has negligible advantage.

Theorem 2. *Suppose that there exists a PPT attacker $\mathcal{A}$ against the sID-IND-CPA security of the Boneh-Boyen HIBE that makes at most q_K `Corrupt` oracle queries and has advantage $Adv_{\mathcal{A}}^{\texttt{HIBE}}(k)$. Then there exists a PPT algorithm $\mathcal{B}$ that solves the DBDH problem with advantage $Adv_{\mathcal{B}}^{\texttt{BDDH}}(k) \geq Adv_{\mathcal{A}}^{\texttt{HIBE}}(k)/2 - q_K/2p$.*

Proof We directly describe the algorithm $\mathcal{B}$ against the DBDH problem:

1. $\mathcal{B}$ receives the input (g, g^a, g^b, g^c, Z).
2. $\mathcal{B}$ runs $\mathcal{A}_0$ to obtain the challenge coalition $TA^* = \{TA_1^*, \ldots, TA_{n^*}^*\}$ and the challenge identity $ID^* = (ID_0^*, \ldots, ID_{\ell^*}^*)$ under the challenge trust authority $ID_0^* = TA_1^*$ (wlog).
3. If $\ell^* < L$ then $\mathcal{B}$ randomly generates $ID_{\ell^*+1}^*, \ldots, ID_L^* \xleftarrow{\$} \mathbb{Z}_p$.
4. $\mathcal{B}$ computes the challenge parameters

$$g_1 \leftarrow g \qquad g_2 \leftarrow g^b \qquad k_{i,j}, \alpha_j \xleftarrow{\$} \mathbb{Z}_p^* \text{ for } 0 \leq i \leq L, j \in \{0,1\}$$
$$pk_1 \leftarrow g^a / g^{\sum_{j=2}^{n^*} \alpha_j} \qquad pk_j \leftarrow g^{\alpha_j} \text{ and } sk_j \leftarrow (g^b)^{\alpha_j} \text{ for } 2 \leq j \leq n^*$$
$$u_{i,0} \leftarrow g_1^{k_{i,0}} \cdot (g^a)^{-ID_i^* k_{i,1}} \qquad u_{i,1} \leftarrow (g^a)^{k_{i,1}} \qquad \text{for } 0 \leq i \leq L$$

5. $\mathcal{B}$ runs $\mathcal{A}_1$ on the input $(g_1, g_2, u_{0,0}, u_{0,1}, \ldots, u_{L,0}, u_{L,1}, PK)$ where $PK = (pk_1, \ldots, pk_{n^*})$. If $\mathcal{A}_1$ makes an oracle query, then $\mathcal{B}$ answers queries as follows:
   - `CreateTA`: $\mathcal{B}$ generates $\alpha_{TA} \xleftarrow{\$} \mathbb{Z}_p$ and returns the public key $g_1^{\alpha_{TA}}$, while storing α_{TA} for future use. Note that $\mathcal{B}$ knows the private key for all TAs except TA_1^*. Hence, we only have to show how to simulate the remaining oracles for TA_1.
   - `SubmitTA`: $\mathcal{B}$ ignores any queried made to this oracle (as the Boneh-Boyen scheme does not make use of public key values in the `CoalitionBroadcast` algorithm).

– `Corrupt`: Suppose $\mathcal{A}$ requests the decryption key for $(TA^*_1, ID_1 \ldots, ID_\ell)$. If ID is not ancestor of $(TA^*_1, ID^*_1, \ldots, ID^*_L)$, then there exists an index $1 \leq \mu \leq \ell$ such that $ID_\mu \neq ID^*_\mu$. $\mathcal{B}$ generates $r_1, \ldots, r_\mu \xleftarrow{\$} \mathbb{Z}_p$ and computes the decryption key $(h, a_0, \ldots, a_\mu)$ for $(ID_0, \ldots, ID_\mu)$ as

$$\begin{aligned} h &\leftarrow g_2^{-\frac{k_{\mu,0}}{k_{\mu,1}(ID_\mu - ID^*_\mu)}} \cdot g_2^{-\sum_{j=2}^{n^*}\alpha_j} \cdot \prod_{i=0}^{\mu}\left(u_{i,0} \cdot u_{i,1}^{ID_i}\right)^{r_i} \\ a_i &\leftarrow g_1^{r_i} \text{ for } 0 \leq i \leq \mu - 1 \\ a_\mu &\leftarrow g_2^{-\frac{1}{k_{\mu,1}(ID_\mu - ID^*_\mu)}} \cdot g_1^{r_j}\,. \end{aligned}$$

$\mathcal{B}$ computes the decryption key for ID using the key derivation algorithm and returns the result. If no such μ exists (i.e. if ID is an ancestor of $(TA^*_1, ID^*_1, \ldots, ID^*_L)$ then $\mathcal{B}$ aborts .

– `CoalitionBroadcast`: Suppose that $\mathcal{A}$ makes a request for TA^*_1 to send messages to the coalition $\mathcal{C}$. $\mathcal{B}$ generates $r_1 \xleftarrow{\$} \mathbb{Z}_p$ and computes for each $TA_i \in \mathcal{C} \setminus \{TA\}$

$$\begin{aligned} w_{i,0} &\leftarrow g_2^{-\frac{k_{1,0}}{k_{1,1}(TA_i - TA^*_1)}} \cdot g_2^{-\sum_{j=2}^{n^*}\alpha_j} \cdot \left(u_{1,0} \cdot u_{1,1}^{TA_i}\right)^{r_1} \\ w_{i,1} &\leftarrow g_2^{-\frac{1}{k_{1,1}(TA_i - TA^*_1)}} g_1^{r_1} \end{aligned}$$

and sets $w_j \leftarrow (w_{j,0}, w_{j,1})$. $\mathcal{B}$ returns the list $\{w_j : TA_j \in \mathcal{C} \setminus \{TA\}\}$.

– `CoalitionUpdate`: The output of this oracle can be returned directly as it is independent of any private key values.

– `Encrypt`: Suppose $\mathcal{A}_1$ makes the oracle query on two equal-length messages (m_0, m_1). $\mathcal{B}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$ and computes the ciphertext

$$C^* \leftarrow (g^c, (g^c)^{k_{1,0}}, \ldots, (g^c)^{k_{\ell^*,0}}, m_b \cdot Z)\,.$$

$\mathcal{A}_1$ terminates with the output of a bit b'.

6. If $b = b'$ then $\mathcal{B}$ outputs 1. Otherwise, outputs 0.

The `Corrupt` oracle for subordinates works perfectly provided that $\mathcal{A}_1$ does not abort, which can only occur if $\mathcal{A}_1$ makes query on an identity ID which is not an ancestor of ID^* but is an ancestor of $(ID^*_0, \ldots, ID^*_L)$. This can only occur if $\ell > \ell^*$ and $ID_{\ell^*+1} = ID^*_{\ell^*+1}$, which occurs with probability $1/p$ as this value is information theoretically hidden from $\mathcal{A}$. Hence, the probability that this does not occur in the entire execution of $\mathcal{A}$ is q_K/p where q_K is the number of queries to the `Corrupt` oracle. We note that the corrupt oracle gives correct responses for queries since

$$sk_1 \left(u_{j,0} \cdot u_{j,1}^{ID_j}\right)^r = g_2^{\frac{-k_{j,0}}{k_{j,1}(ID_j - ID^*_j)}} \cdot g_2^{-\sum_{i=2}^{n^*}\alpha_i} \qquad \text{for} \qquad r = -\frac{b}{k_{j,1}(ID_j - ID^*_j)}\,.$$

A similar calculation shows that the `CoalitionBroadcast` algorithm gives correct broadcast messages for TA^*_1. All other oracles that $\mathcal{B}$ provides correctly simulate the security model for $\mathcal{A}$.

If $Z = e(g, g)^{abc}$ then the challenge ciphertext is a correct encryption of m_b. This is because an encryption using the random value c would have

$$\begin{gathered} C_1 = g_1^c = g^c \\ C_{2,i} = (u_{i,0} \cdot u_{i,1}^{ID^*_i})^c = (g^c)^{k_{i,0}} \qquad \text{for } 0 \leq i \leq \ell^* \\ C_3 = m_b \cdot e(\textstyle\prod_{i=0}^{n^*} pk_i, g_2)^c = m_b \cdot e(g^a, g^b)^c = m_b \cdot e(g, g)^{abc} \end{gathered}$$

The probability that $\mathcal{B}$ outputs 1 in this situation is the probability that $b = b'$ in the sID-IND-CPA game for the attacker $\mathcal{A}$. This probability can be shown to be $(Adv^{\mathtt{HIBE}}_{\mathcal{A}}(k) - 1)/2$. If Z is random then the challenge ciphertext information theoretically hides b and so the probability that $\mathcal{B}$ outputs 1 in this situation is $1/2$. This completes the proof. $\square$

4 Strengthened Security Results

4.1 IND-CPA Security

We may prove the security of the Boneh-Boyen scheme in the (non-selective-identity) IND-CPA model by hashing all identities before use. The proof of this fact mirrors the proof in Abdalla *et al.* [?] (in the random oracle model).

4.2 IND-CCA2 Security

We may transform an IND-CPA MTA-WIBE scheme into an IND-CCA2 MTA-WIBE scheme using the CHK transform [?] in a manner similar to that described in Abdalla *et al.* [?]. However, we will describe an alternative transformation based on the Boneh-Katz (BK) transform [?]. This gives a new and more efficient method to transform IND-CPA secure WIBEs into IND-CCA2 secure WIBEs.

Boneh-Katz transforms an MTA-WIBE $\mathit{\Pi}$ into a new MTA-WIBE $\mathit{\Pi}'$ using a MAC algorithm $\textsc{Mac}$ and an "encapsulation" scheme $(\mathcal{G}, \mathcal{S}, \mathcal{R})$. The encapsulation scheme has a key generation algorithm $\sigma \xleftarrow{\$} \mathcal{G}(1^k)$, commitment algorithm $(K, com, dec) \xleftarrow{\$} \mathcal{S}(1^k, \sigma)$, and a decommitment algorithm $\mathcal{D}(\sigma, com, dec)$ which outputs either a bitstring K or the error symbol $\perp$. We assume that $K \in \{0,1\}^k$. We require that if $(K, com, dec) \xleftarrow{\$} \mathcal{S}(1^k, \sigma)$ then $\mathcal{D}(\sigma, com, dec) = K$. We also require that the scheme is hiding in the sense that for all PPT attackers $\mathcal{A}$ have negligible advantage:

$$\left| \Pr\left[\mathcal{A}(1^k, \sigma, com, K_b) = b \;:\; \begin{array}{c} \sigma \xleftarrow{\$} \mathcal{G}(1^k);\; K_0 \xleftarrow{\$} \{0,1\}^k \\ (K_1, com, dec) \xleftarrow{\$} \mathcal{S}(1^k, \sigma);\; b \xleftarrow{\$} \{0,1\} \end{array} \right] - \frac{1}{2} \right|$$

We further require that the encapsulation scheme is binding in the sense that for all PPT attackers $\mathcal{A}$ have negligible advantage:

$$\Pr\left[\mathcal{R}(\sigma, com, dec') \notin \{\perp, K\} \;:\; \begin{array}{c} \sigma \xleftarrow{\$} \mathcal{G}(1^k);\; (K, com, dec) \xleftarrow{\$} \mathcal{S}(1^k, \sigma) \\ dec' \xleftarrow{\$} \mathcal{A}(1^k, \sigma, K, com, dec) \end{array} \right]$$

Lastly, we assume that the decommitments dec^* are always of some fixed size (which may depend on k). The security notions for a MAC scheme are given in Appendix A.2. The transform of $\mathit{\Pi}$ into $\mathit{\Pi}'$ is given in Figure 2. We assume that "$-$" represents some fixed, publicly-known allowable identity for the CPA scheme; we will deliberately exclude "$-$" from the space of allowable identities in the CCA scheme.

Theorem 3. *Suppose that the $\mathit{\Pi}$ is an IND-CPA secure MTA-WIBE,* $\textsc{Mac}$ *is an unforgeable MAC scheme, and $(\mathcal{G}, \mathcal{S}, \mathcal{R})$ is a hiding and binding encapsulation algorithm. Then the MTA-WIBE $\mathit{\Pi}'$ produced by the BK transform is IND-CCA2 secure.*

The proof strategy is similar to that of Boneh and Katz [?] but has to deal with technical details introduced by the trust authorities and the WIBE scheme. A full proof is given in Appendix C.

4.3 Optimized BK for the Boneh-Boyen MTA-WIBE

In the particular case where we apply the BK transform to the BB MTA-WIBE, we can optimize the transform to obtain an efficient sID-IND-CCA2 secure MTA-WIBE. The optimization comes from several points:

- It is possible to extract a coalition key for an identity $ID \| ID'$ from c_{ID} and ID' using the same technique as for the derivation of decryption key d_{ID}. Hence we can run the `CoalitionExtract` algorithm as part of `CoalitionExtract`$'$ algorithm, rather than as part of the `Decrypt`$'$ oracle. This improves efficiency.

```
Setup'(1^k):
  $param \xleftarrow{\$} \texttt{Setup}(1^k)$
  $\sigma \xleftarrow{\$} \mathcal{G}(1^k)$
  $param' \leftarrow (param, \sigma)$
  Return $param'$

Encode(P, α):
  Parse $P$ as $(P_0, \ldots, P_\ell)$
  For $i = 0, \ldots, \ell$, $P'_i \leftarrow P_i$
  For $i = \ell + 1, \ldots, L$, $P'_i \leftarrow$ "–"
  $P'_{L+1} \leftarrow \alpha$
  Return $P'$

Encode'(P, ID, α):
  For $i = 1, \ldots, |P| - |ID|$
    If $P_{|ID|+i} \neq *$ then $ID'_i \leftarrow P_{|ID|+i}$
    If $P_{|ID|+i} = *$ then $ID'_i \leftarrow 1^k$
  For $i = 1, \ldots, L - |P|$
    $ID_{|P|-|ID|+i} \leftarrow$ "–"
  $ID_{L-|ID|+1} \leftarrow \alpha$
  Return $ID'$

CoalitionExtract'(d_ID, v):
  $c_{ID} \leftarrow (d_{ID}, v)$
  Return $c_{ID}$

Encrypt'(C, PK, P, m):
  $(K, com, dec) \xleftarrow{\$} \mathcal{S}(1^k, \sigma)$
  $P' \leftarrow \texttt{Encode}(P, com)$
  $m' \leftarrow (m, dec)$
  $C' \xleftarrow{\$} \texttt{Encrypt}(\mathcal{C}, PK, P', m')$
  $\tau \leftarrow \textsc{Mac}_K(\mathcal{C} \| P \| C')$
  Return $(com, \mathcal{C}, P, C', \tau)$

Decrypt'(c_ID, C):
  Parse $C$ as $(com, \mathcal{C}, P, C', \tau)$
  Parse $c_{ID}$ as $(d_{ID}, v)$
  $ID' \leftarrow \texttt{Encode}'(P, ID, com)$
  $d' \xleftarrow{\$} \texttt{Extract}(ID, d_{ID}, ID')$
  $c' \leftarrow \texttt{CoalitionUpdate}(d', v)$
  $(m, dec) \xleftarrow{\$} \texttt{Decrypt}(c, C')$
  $K \leftarrow \mathcal{R}(\sigma, com, dec)$
  If $\textsc{Mac}_K(\mathcal{C} \| P \| C') \neq \tau$ then return $\perp$
  Else return $m$
```

Fig. 2. The Boneh-Katz transform for a MTA-WIBE. Any algorithm of Π' not explicitly defined in this figure is identical to the corresponding algorithm in Π. The `Encode` algorithm turns an ℓ level pattern into an $L + 1$ level pattern. The `Encode'` algorithm computes the extension to ID required to turn an identity which matches P into an identity which matches `Encode`(P, α).

– The BB MTA-WIBE is level independent in the sense that we can specify an identifier for level L (and extract a decryption key which only works for that identifier at that level) without needing to specify an identifier for the levels $1 \leq i < L$. Hence, we can specify a ciphertext with $C_{2,L} \leftarrow (u_{L,0} \cdot u_{L,1}^{com^*})^t$ without needing to specify ciphertexts $C_{2,i} \leftarrow (u_{i,0} \cdot u_{i,1}^{\text{"–"}})^t$ for $|P| < i < L$. This removes the need for the `Encode` and `Encode'` algorithms, improves efficiency, and reduces bandwidth.

The (random-oracle-based) selective-identity to non-selective-identity transform can then be applied to the sID-IND-CCA2 scheme to give a IND-CCA2 secure scheme.

References

1. M. Abdalla, D. Catalano, A. W. Dent, J. Malone-Lee, G. Neven, and N. P. Smart. Identity-based encryption gone wild. In M. Bugliesi, Bart Preneel, V. Sassone, and I. Wegener, editors, *Automata, Languages and Programming – ICALP 2006*, volume 4052 of *Lecture Notes in Computer Science*, pages 300–311. Springer-Verlag, 2006.
2. K. D. Boklan, Z. Klagsbrun, K. G. Paterson, and S. Srinivasan. Flexible and secure communications in an identity-based coalition environment. In *Proc. IEEE Military Communications Conference - MILCOM 2008*, 2008.
3. D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – Eurocrypt 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2004.
4. D. Boneh and J. Katz. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In A. Menezes, editor, *Topics in Cryptology – CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 87–103. Springer-Verlag, 2005.
5. R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – Eurocrypt 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222. Springer-Verlag, 2004.

6. J. Horwitz and B. Lynn. Towards hierarchical identity-based encryption. In L. Knudsen, editor, *Advance in Cryptology – Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer-Verlag, 2002.
7. K. G. Paterson and S. Srinivasan. Security and anonymity of identity-based encryption with multiple trusted authorities. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 354–375. Springer-Verlag, 2008.
8. A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology – Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.

A Standard Definitions

A.1 Algorithms and Assignment

Throughout this article, $y \leftarrow x$ denotes the assignment of the value x to the variable y and $y \xleftarrow{\$} S$ denotes the assignment of a uniform random element of the finite set S to the variable y. If $\mathcal{A}$ is a probabilistic algorithm, then $y \xleftarrow{\$} \mathcal{A}(x)$ denotes the assignment of the output of the algorithm $\mathcal{A}$ run on the input x to the variable y when $\mathcal{A}$ is computed using a fresh set of random coins. We write $y \leftarrow \mathcal{A}(x)$ if $\mathcal{A}$ is deterministic.

A.2 MAC algorithms

A MAC algorithm is a deterministic polynomial-time algorithm Mac. It takes as input a message $m \in \{0,1\}^*$ and a symmetric key $K \in \{0,1\}^k$, and outputs a tag $\tau \leftarrow \textsc{Mac}_K(m)$. It should be infeasible for a PPT attacker $\mathcal{A}$ to win the unforgeability game: (1) the challenger generates a key $K \xleftarrow{\$} \{0,1\}^*$; (2) the attacker outputs a forgery $(m^*, \tau^*) \xleftarrow{\$} \mathcal{A}(1^k)$. During its execution the attacker can query a MAC oracle with a message m and will receive $\textsc{Mac}_K(m)$. The attacker wins if $\textsc{Mac}_K(m^*) = \tau^*$ and m^* was never queried to the MAC oracle. The attackers probability of winning is written $Adv_{\mathcal{A}}^{\texttt{MAC}}(k)$.

B Security Proof for BB-WIBE to BB-HIBE Reduction

Proof of Theorem 1

We directly describe the algorithm $\mathcal{B}$ which breaks the HIBE using the algorithm $\mathcal{A}$ as a subroutine. Before we begin, we define some useful notation. If $P = (P_1, \ldots, P_k)$ is a pattern, then

$$W(P) = \{1 \le i \le k : P_i = *\} \quad \text{and} \quad W(P_{\le j}) = \{1 \le i \le \min\{j,k\} : P_i = *\}\,.$$

The algorithm $\mathcal{B}$ runs as follows:

1. $\mathcal{B}$ runs $\mathcal{A}_0$ on the security parameter. $\mathcal{A}_0$ responds by outputting a description of the challenge coalition $TA^* = (TA_1^*, \ldots, TA_n^*)$ and the challenge pattern $P^* = (P_1^*, \ldots, P_{\ell^*}^*)$. Let π be a map which identifies the number of non-wildcard entries in the first i layers of P^*, i.e. $\pi(i) = i - |W(P^*_{\le i})|$. $\mathcal{B}$ outputs the challenge coalition TA^* and the challenge identity $\hat{ID}^* = (\hat{ID}_1^*, \ldots, \hat{ID}_{\pi(\ell^*)}^*)$ where $\hat{ID}_{\pi(i)}^* = P_i^*$ for $i \notin W(P^*)$.
2. $\mathcal{B}$ responds with HIBE parameters $param = (\hat{g}_1, \hat{g}_2, \hat{u}_{1,0}, \ldots, \hat{u}_{L,1})$. $\mathcal{B}$ generates WIBE parameters as follows:
$$\begin{aligned} (g_1, g_2) &\leftarrow (\hat{g}_1, \hat{g}_2) \\ u_{i,j} &\leftarrow \hat{u}_{\pi(i),j} && \text{for } i \notin W(P^*), j \in \{0,1\} \\ u_{i,j} &\leftarrow g_1^{\beta_{i,j}} && \text{for } i \in W(P^*), j \in \{0,1\} \text{ where } \beta_{i,j} \xleftarrow{\$} \mathbb{Z}_p \\ u_{i,j} &\leftarrow \hat{u}_{i-|W(P^*)|,j} && \text{for } i \in \{\ell^*+1, \ldots, L\}, j \in \{0,1\}\,. \end{aligned}$$
3. $\mathcal{B}$ executes $\mathcal{A}_1$ on the public parameters $(g_1, g_2, u_{0,0}, \ldots, u_{L,1})$. $\mathcal{A}$ may make the following oracle queries:
   – `CreateTA`: $\mathcal{B}$ forwards this request to its own oracle and returns the response.
   – `SubmitTA`: $\mathcal{B}$ may ignore these queries as the `CoalitionBroadcast` algorithm does not depend upon individual TA's public keys.

– `CoalitionBroadcast`: $\mathcal{B}$ forwards this request to its own oracle and returns the response.
– `CoalitionKeys`: $\mathcal{B}$ forwards this request to its own oracle and returns the response.
– `Corrupt`: To extract a decryption key for an identity $ID = (ID_1, \ldots, ID_\ell)$ which does not match the challenge pattern, $\mathcal{B}$ computes the projection of the identity onto the HIBE identity space to give a projected identity $\hat{ID} = (\hat{ID}_1 \ldots, \hat{ID}_{\hat{\ell}})$.
  - If $\ell \leq \ell^*$ then $\hat{\ell} \leftarrow \pi(\ell)$ and $\hat{ID}_{\pi(i)} \leftarrow ID_i$ for $i \notin W(P^*_{\leq \ell})$. Since ID does not match the challenge pattern for the WIBE, $\hat{ID}$ does not match the challenge identity for the HIBE. $\mathcal{B}$ queries its `Corrupt` oracle on $\hat{ID}$ and receives $(\hat{h}, \hat{a}_0, \ldots, \hat{a}_{\hat{\ell}})$ in response. $\mathcal{B}$ now "retro-fits" to find a complete key, by setting
$$\begin{array}{ll} a_0 \leftarrow \hat{a}_0 & \\ a_i \leftarrow \hat{a}_{\pi(i)} & \text{for } 1 \leq i \leq \ell \text{ and } i \notin W(P^*_{\leq \ell}) \\ a_i \leftarrow g_1^{r_i} & \text{for } 1 \leq i \leq \ell \text{ and } i \in W(P^*_{\leq \ell}) \text{ where } r_i \xleftarrow{\$} \mathbb{Z}_p \\ h \leftarrow \hat{h} \prod_{i=1, i \in W(P^*_{\leq \ell})}^{\ell} (u_{i,0} \cdot u_{i,1}^{ID_i})^{r_i} & \end{array}$$
and returning the key $(h, a_0, \ldots, a_\ell)$.
  - If $\ell > \ell^*$, then $\hat{\ell} = \ell - |W(P^*)|$, $\hat{ID}_{\pi(i)} \leftarrow ID_i$ for $1 \leq i \leq \ell^*$ and $i \notin W(P^*)$, and $\hat{ID}_{i-|W(P^*)|} \leftarrow ID_i$ for $\ell^* < i \leq \ell$. Since ID does not match the challenge pattern for the WIBE, $\hat{ID}$ does not match the challenge identity for the HIBE. $\mathcal{B}$ queries its `Corrupt` oracle on $\hat{ID}$ and receives $(\hat{h}, \hat{a}_0, \ldots, \hat{a}_{\hat{\ell}})$ in response. $\mathcal{B}$ now "retro-fits" to find a complete key, by setting
$$\begin{array}{ll} a_0 \leftarrow \hat{a}_0 & \\ a_i \leftarrow \hat{a}_{\pi(i)} & \text{for } 1 \leq i \leq \ell^* \text{ and } i \notin W(P^*) \\ a_i \leftarrow g_1^{r_i} & \text{for } 1 \leq i \leq \ell^* \text{ and } i \in W(P^*) \text{ where } r_i \xleftarrow{\$} \mathbb{Z}_p \\ a_i \leftarrow \hat{a}_{i-|W(P^*)|} & \text{for } \ell^* < i \leq \ell \\ h \leftarrow \hat{h} \prod_{i=1, i \in W(P^*)}^{\ell^*} (u_{i,0} \cdot u_{i,1}^{ID_i})^{r_i} & \end{array}$$
and returning the key $(h, a_0, \ldots, a_\ell)$.

– `Encrypt`: $\mathcal{A}$ outputs two equal-length messages (m_0, m_1). $\mathcal{B}$ queries its own encryption oracle on the messages (m_0, m_1) and receives the ciphertext $(C_1^*, \hat{C}_{2,1}^*, \ldots, \hat{C}_{2,\pi(\ell^*)}^*, C_3^*)$. $\mathcal{B}$ retro-fits this to form the challenge ciphertext for $\mathcal{A}$ by setting
$$\begin{array}{ll} C_{2,i}^* \leftarrow \hat{C}_{2,\pi(i)}^* & \text{for } 1 \leq i \leq \ell^*, i \notin W(P^*) \\ C_{2,i}^* \leftarrow (C_1^{*\beta_{i,0}}, C_1^{*\beta_{i,1}}) & \text{for } 1 \leq i \leq \ell^*, i \in W(P^*) \,. \end{array}$$

$\mathcal{A}_1$ terminates with the output of a bit b'.

4. $\mathcal{B}$ outputs the bit b'.

The algorithm $\mathcal{B}$ correctly simulates the oracles to which $\mathcal{A}$ has access; furthermore, $\mathcal{B}$ wins the HIBE game if and only if $\mathcal{A}$ wins the game. Hence, the theorem is proven. □

C Security Proof for the BK Transform

Proof of Theorem 3

Our proof proceeds through a series of games. Let W_i be the event that the attacker $\mathcal{A}$ outputs $b' = b$ in Game i and let starred values denote values computed during the computation of the challenge ciphertext. Let Game 1 be the normal IND-CCA2 game for $\mathcal{A}$. Hence,
$$Adv_{\mathcal{A}}^{\texttt{CCA}}(k) = 2 \cdot |\Pr[W_1] - 1/2| \,.$$
Let Game 2 be the same as Game 1 except that $\mathcal{A}$ is deemed to lose if it submits a ciphertext (com^*, P, C, τ) such that the decommitment value dec' recovered during the decryption process satisfies $\mathcal{R}(\sigma, com, dec') \notin \{\perp, K^*\}$. It is easy to show that there exists a PPT algorithm $\mathcal{B}$ such that $|\Pr[W_1] - \Pr[W_2]| \leq Adv_{\mathcal{B}}^{\texttt{bind}}(k)$.

Let Game 3 be identical to Game 2 except that the encryption oracle computes $m'^* \leftarrow (m_b, 0^{|dec^*|})$ rather than $m'^* \leftarrow (m_b, dec^*)$. Let E_2 be the event that $\mathcal{A}$ submits a ciphertext $(com^*, \mathcal{C}, P, C', \tau)$ to the decryption oracle with $\textsc{Mac}_{K^*}(\mathcal{C}\|P\|C') = \tau$ in Game 2. Let E_3 be the event that $\mathcal{A}$ submits a ciphertext $(com^*, \mathcal{C}, P, C', \tau)$ to the decryption oracle with $\textsc{Mac}_{K^*}(\mathcal{C}\|P\|C') = \tau$ in Game 3. There exists an algorithm $\mathcal{B}^*$ against the IND-CPA security of Π such that $|\Pr[E_3] - \Pr[E_2]| \le Adv^{\texttt{CPA}}_{\mathcal{B}^*}(k)$. The attacker $\mathcal{B}^*(param)$ is defined as follows:

1. $\sigma \xleftarrow{\$} \mathcal{G}(1^k)$ and $(K^*, com^*, dec^*) \xleftarrow{\$} \mathcal{S}(1^k, \sigma)$.
2. $param' \leftarrow (param, \sigma)$.
3. Run $b' \xleftarrow{\$} \mathcal{A}(param')$. Suppose $\mathcal{A}$ makes an oracle query.
   - If $\mathcal{A}$ makes a `CreateTA`, `SubmitTA`, `CoalitionBroadcast`, `CoalitionUpdate`, `CoalitionExtract` or `Corrupt` query, then $\mathcal{B}^*$ passes the query to its own oracle and returns the result.
   - If $\mathcal{A}$ makes an encryption oracle query on the equal-length messages (m_0, m_1), the pattern P^*, and the coalition $\mathcal{C}^*$ then $\mathcal{B}^*$ computes $P'^* \leftarrow \texttt{Encode}(P^*, com^*)$, $d \xleftarrow{\$} \{0,1\}$, $m'_0 \leftarrow (m_d, dec^*)$, $m'_1 \leftarrow (m_d, 0^{|dec^*|})$, and queries its encryption oracle on (m'_0, m'_1), the pattern P'^*, and the coalition $\mathcal{C}^*$. It receives C'^* from its oracle, and computes $\tau^* \leftarrow \textsc{Mac}_{K^*}(\mathcal{C}^*\|P^*\|C'^*)$. It returns $(com^*, \mathcal{C}^*, P^*, C'^*, \tau^*)$.
   - If $\mathcal{A}$ makes a decryption query on $(com, \mathcal{C}, P, C', \tau)$ with $com \neq com^*$ for the identity ID and the coalition $\mathcal{C}$, then $\mathcal{B}^*$ computes $P' \leftarrow \texttt{Encode}(P, com)$, replaces the wildcards in P' with 1^k to form the identity ID' and requests the decryption key $d_{ID'}$ for ID'. Since $\mathcal{A}$ can only make decryption queries for coalitions for which the adjustment parameter v is known, $\mathcal{B}^*$ forms the decryption key $c' \xleftarrow{\$} \texttt{CoalitionExtract}(d_{ID'}, v)$. $\mathcal{B}^*$ can use this key to decrypt C', and decrypt the rest of the ciphertext as normal.
   - If $\mathcal{A}$ makes a decryption query on $(com^*, \mathcal{C}, P, C', \tau)$, then $\mathcal{B}^*$ checks whether $\textsc{Mac}_{K^*}(\mathcal{C}\|P\|C') = \tau$. If so, $\mathcal{B}^*$ outputs 1 and terminates. Otherwise, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
4. $\mathcal{B}^*$ outputs 0

This attacker is legal since it only queries the decryption oracle on identities with $com \neq com^*$. If $b = 0$ then $\mathcal{B}^*$ outputs 1 whenever E_2 occurs. If $b = 1$ then $\mathcal{B}^*$ outputs 1 whenever E_3 occurs. Hence, $|Pr[E_3] - \Pr[E_2]| \le Adv^{\texttt{CPA}}_{\mathcal{B}^*}(k)$.

There exists an attacker $\mathcal{B}'$ such that $|\Pr[W_3|\neg E_3] - \Pr[W_2|\neg E_2]| \le Adv^{\texttt{CPA}}_{\mathcal{B}'}(k)$. The attacker $\mathcal{B}'(param)$ is defined as follows:

1. $\sigma \xleftarrow{\$} \mathcal{G}(1^k)$ and $(K^*, com^*, dec^*) \xleftarrow{\$} \mathcal{S}(1^k, \sigma)$.
2. $param' \leftarrow (param, \sigma)$.
3. Run $d' \xleftarrow{\$} \mathcal{A}(param')$. Suppose $\mathcal{A}$ makes an oracle query.
   - If $\mathcal{A}$ makes a `CreateTA`, `SubmitTA`, `CoalitionBroadcast`, `CoalitionUpdate`, `CoalitionExtract` or `Corrupt` query, then $\mathcal{B}$ passes the query to its own oracle and returns the result.
   - If $\mathcal{A}$ makes an encryption oracle query on the equal-length messages (m_0, m_1) and the pattern P^*, then $\mathcal{B}$ computes $P'^* \leftarrow \texttt{Encode}(P^*, com^*)$, $d \xleftarrow{\$} \{0,1\}$, $m'_0 \leftarrow (m_d, dec^*)$, $m'_1 \leftarrow (m_d, 0^{|dec^*|})$, and queries its encryption oracle on (m'_0, m'_1) and the pattern P'. It receives C'^* from its oracle, and computes $\tau^* \leftarrow \textsc{Mac}_{K^*}(\mathcal{C}^*\|P'^*\|C'^*)$. It returns $(com^*, \mathcal{C}^*, P^*, C'^*, \tau^*)$.
   - If $\mathcal{A}$ makes a decryption query on $(com, \mathcal{C}, P, C', \tau)$ with $com \neq com^*$ for the identity ID and the coalition $\mathcal{C}$, then $\mathcal{B}$ computes $P' \leftarrow \texttt{Encode}(P, com)$, replaces the wildcards in P' with 1^k to form the identity ID' and requests the decryption key $d_{ID'}$ for ID'. Since $\mathcal{A}$ can only make decryption queries for coalitions for which the adjustment parameter v is known, $\mathcal{B}$ forms the decryption key $c' \xleftarrow{\$} \texttt{CoalitionExtract}(d_{ID'}, v)$. $\mathcal{B}$ can use this key to decrypt C', and decrypt the rest of the ciphertext as normal.
   - If $\mathcal{A}$ makes a decryption query on $(com^*, \mathcal{C}, P, C', \tau)$, then $\mathcal{B}$ returns $\perp$.
4. If $d = d'$ then $\mathcal{B}'$ returns 1, else it returns 0.

This is a legal attacker and $|\Pr[W_3|\neg E_3] - \Pr[W_2|\neg E_2]| \le Adv^{\texttt{CPA}}_{\mathcal{B}'}(k)$. A simple probability argument can be used to show that:

$$|\Pr[W_3] - \Pr[W_2]| \le 2 \cdot Adv^{\texttt{CPA}}_{\mathcal{B}^*}(k) + Adv^{\texttt{CPA}}_{\mathcal{B}'}(k) + \Pr[E_3]\,.$$

Next, let Game 4 be identical to Game 3 except that the key K^* used in the encryption algorithm (and to determine if ciphertexts should be rejected) is randomly chosen from $\{0,1\}^k$. There exists an attacker $\mathcal{B}^\dagger$ against the hiding property of the encapsulation algorithm such that $|\Pr[W_4] - \Pr[W_3]| \leq 2 \cdot Adv^{\mathtt{hide}}_{\mathcal{B}^\dagger}(k)$. Let E_4 be the event that $\mathcal{A}$ submits a ciphertext $(com^*, \mathcal{C}, P, C', \tau)$ to the decryption oracle with $\textsc{Mac}_{K^*}(\mathcal{C}\|P\|C') = \tau$ in Game 4. Again, we have $|\Pr[E_4] - \Pr[E_3]| \leq 2 \cdot Adv^{\mathtt{hide}}_{\mathcal{B}^\dagger}(k)$.

Finally, let Game 5 be identical to Game 4 except that (a) the attacker loses if it queries the decryption oracle on a ciphertext $(com^*, \mathcal{C}, P, C', \tau)$ before it queries the encryption oracle, and (b) the attacker returns $\perp$ whenever the attacker queries the decryption oracle on a ciphertext $(com^*, \mathcal{C}, P, C', \tau)$ after it queries the encryption oracle. There exists an algorithm $\mathcal{B}''$ against the MAC algorithm such that $|\Pr[W_5] - \Pr[W_4]| \leq q_D Adv^{\mathtt{MAC}}_{\mathcal{B}''}(k) + \gamma(k)$ where $\gamma(k)$ is the maximum probability that a randomly generated com^* is any fixed binary value. As a byproduct, we also obtain $\Pr[E_4] \leq q_D Adv^{\mathtt{MAC}}_{\mathcal{B}''}(k)$.

We can show a direct reduction from Game 5 to the underlying IND-CPA security of $\mathit{\Pi}$. There exists an algorithm $\mathcal{B}^\sharp$ such that $2 \cdot |\Pr[W_5] - 1/2| = Adv^{\mathtt{CPA}}_{\mathcal{B}^\sharp}(k)$. This algorithm simply translates decryption oracle queries made by $\mathcal{A}$ against the MTA-WIBE scheme into translates decryption oracles made by $\mathcal{B}^\sharp$ against the tag-based encryption scheme (for ciphertexts with $com \neq com^*$) or returns $\perp$ (for ciphertexts with $com = com^*$). All decryption oracle queries made by $\mathcal{B}^\sharp$ are legal as the weak selective-tag IND-CPA security model allows for decryption oracle queries for tags $com \neq com^*$. This concludes the proof. $\square$