Proof of Security

Charting the Course

Proof of security in two steps. We will base multi-TA WIBE security (IND-smWID-CPA) on multi-TA HIBE security (IND-smID-CPA), which in turn will be based on the Bilinear Decision Diffie-Hellman problem (BDDH). In the construction of this Boneh-Boyen-based scheme, each TA_j has a private key $d_j = (\Sigma\alpha_i \cdot g_2 + \Sigma r_{i,j}(u_{0,0} + ID_{j,1} \cdot u_{0,1}), \Sigma r_{i,j} \cdot g_1)$ with summations over $i \in \{1 \ldots n\}$. These keys are constructed by taking input from each TA_i of the form (α_i)

HIBE to WIBE

Theorem:

If the Boneh-Boyen multi-*TA* HIBE is IND-smID-CPA secure then its respective WIBE is IND-smWID-CPA secure.

Proof:

The proof will follow by contradiction. Assume an adversary $\mathcal{A}$ with an advantage in the IND-smID-CPA game for the WIBE. We will construct another adversary $\mathcal{B}$ which, using $\mathcal{A}$ as a black box, will gain an advantage in the IND-sID-CPA game for the HIBE.

Initialization:

The challenger announces to $\mathcal{B}$ a set of n TA's $(TA_1, \ldots, TA_n)$ and a maximum hierarchy depth L. $\mathcal{B}$ begins interacting with $\mathcal{A}$ and repeats the TA's and depth to $\mathcal{A}$ verbatim. $\mathcal{A}$ responds with a challenge identity $P^* = (P_1, \ldots, P_K)$ with $P_1 \in \{TA_1, \ldots, TA_n\}$ or $P_1 = " * "$. Since $\mathcal{B}$ cannot have any wildcards in his challenge identity we will take the non-wildcard portions of P^* to make a fixed identity ID^*. We set $\mathcal{B}$'s challenge identity to be $ID^* = ID_i^* = P^*_{\pi(i)}$ where the map $\pi(i) = i - |W(P^*_{\leq i})| \forall i \notin W(P^*)$, dropping the wildcard portion. $\mathcal{B}$ announces this ID^* as his choice of challenge identity.

Setup:

The challenger runs `Setup` to generate HIBE parameters $\{g_1, g_2, u_{0,0}, ..., u_{L,1}\}$. Upon receiving these parameters, $\mathcal{B}$ sets his own $\hat{u}_{i,j} = u_{i,j} \forall i \notin W(P)$ and $\hat{u}_{i,j} = g_1 \forall i \in W(P)$ and announces to $\mathcal{A}$ WIBE parameters $\{g_1, g_2, \hat{u}_{0,0}, ... \hat{u}_{L,1}\}$.

Queries:

Any valid query made by $\mathcal{A}$ must be answered by $\mathcal{B}$, possibly after consulting her own oracles. The adversaries $\mathcal{A}$ and $\mathcal{B}$ have the same oracles available: `SetupCoalitionBroadcast`, `SetupCoalitionKeys`, `CorruptTA`, and `CorruptUser`.

Since the TA's available to form coalitions are identical for $\mathcal{A}$ and $\mathcal{B}$, any queries to the `SetupCoalitionBroadcast` and `SetupCoalitionKeys` oracles made by $\mathcal{A}$ may be repeated verbatim by $\mathcal{B}$. Queries made to the `CorruptTA` oracle may be made for any $TA \neq P_1$ when $P_1 \neq "*"$, if the challenge pattern has a wildcard on the TA-level ($P_1 = "*"$) then any TA is an ancestor of the challenge recipient and no `CorruptTA` queries may be made.

Queries to the `CorruptUser` oracle may be made of any node that is not an ancestor of the challenge pattern, i.e. a user $ID = (ID_1, ..., ID_j)$ may not be corrupted if $P_i \in ID_i, "*" \forall i \leq j$. To answer a `CorruptUser` query, $\mathcal{B}$ projects the identity $ID = (ID_1, ID_2, ..., ID_j)$ from the WIBE to the HIBE as $ID' = ID_{\pi(i)}$ and queries her `CorruptUser` oracle for $d_{ID'} = (a_0, a_1, ..., a_{pi(j)})$. $\mathcal{B}$ must now fill in the missing pieces of the key d_{ID}. First $\mathcal{B}$ sets $b_i = a_{\pi^{-1}(i)} \forall i > 0$. Then $\mathcal{B}$ chooses $r_i \leftarrow \mathbb{F}_p$ randomly and sets $b_i = r_i \cdot g_1$ for the missing values of $i > 0$. Finally $\mathcal{B}$ sets the value of $b_0 = a_0 \cdot \Pi r_i (\hat{u}_{i,0} + ID_i \cdot \hat{u}_{i,1})$ and answers $\mathcal{A}$'s query with $d_{ID} = (b_0, b_1, ..., b_j)$.

Challenge:

The final oracle available to both $\mathcal{A}$ and $\mathcal{B}$ is the `Test` oracle, which takes two messages m_0 and m_1 and returns the encrypted m_b for an unknown $b \in \{0, 1\}$. $\mathcal{B}$ allows $\mathcal{A}$ to choose the two messages and passes them on to his `Test` oracle. $\mathcal{B}$ must then remap elements of the ciphertext from the HIBE setting to the WIBE setting, recall the anatomy of a ciphertext C in the HIBE:

$$C_1 = t \cdot g_1$$

$$C_{2,i} = t \cdot (u_{i,0} + (P_i) \cdot u_{i,1})$$

$$C_3 = m \cdot e((\Sigma \alpha_i) \cdot g_1, g_2)^t$$

Note that there are no $C_{4,i,j}$ elements because addresses in the HIBE do not have wildcards. The challenge pattern P^* lives in the WIBE setting and is allowed to contain wildcards, $\mathcal{B}$ must adjust the ciphertext for any wildcards present as follows:

$$
\begin{aligned}
C_1' &= C_1 \\
C_{2,i}' &= C_{2,\pi(i)} \text{ for all } i \notin W(P^*) \\
C_3' &= C_3 \\
C_{4,i,j}' &= C_1 \text{ for all } i \in W(P^*) \text{ and } j \in \{0,1\}
\end{aligned}
$$

This is a valid ciphertext because of our choice of $\hat{u}_{i,j} = g_1$ for all $i \in W(P^*)$. This means that for $i \in W(P^*)$ the value needed for $C_{4,i,j}' = t \cdot u_{i,j} = t \cdot g_1 = C_1$. $\mathcal{B}$ returns this ciphertext to $\mathcal{A}$ as response to the $\mathcal{A}$'s `Test` query. $\mathcal{A}$ responds with a guess of $c \in \{0,1\}$ as the proper value of b, which $\mathcal{B}$ repeats as her guess. Any advantage in the IND-smWID-CPA game that $\mathcal{A}$ has is then transferred onto $\mathcal{B}$.

BDDH to HIBE

Theorem:

If the Bilinear Decisional Diffie-Hellman assumption holds then the multi-*TA* Boneh-Boyen HIBE scheme is IND-smID-CPA secure.

Proof:

We will assume the existence of an adversary $\mathcal{A}$, with non-negligible advantage in the IND-smID-CPA game to construct a new adversary $\mathcal{B}$ who, using $\mathcal{A}$ as a black box, gains a non-negligible advantage in the BDDH game. To start the BDDH game $\mathcal{B}$ is given a 5-tuple $\{g, g^a, g^b, g^c, Z\}$ with $g \in \mathbb{G}_1$ and $Z \in \mathbb{G}_2$, and must decide whether $Z = e(g,g)^{abc}$ or if $Z = e(g,g)^z$ for a random $z \in \mathbb{F}_l$.

Initialization:

$\mathcal{B}$ begins interacting with $\mathcal{A}$ announcing a set of TA's $(TA_1, ..., TA_n)$ available to form coalitions and a maximum hierarchy depth L. $\mathcal{A}$ replies with a challenge identity $ID = (ID_1, ..., ID_j)$ for some $j < L$.

Setup:

$\mathcal{B}$ must construct a multi-*TA* HIBE for $\mathcal{A}$ and give parameters $g_1, g_2, u_{0,0}, u_{1,0}, ..., u_{L,0}, u_{0,1}, u_{1,1}, ..., u_{L,1}$ to $\mathcal{A}$.