Proposal for P1363.3
HIBE, HIBS, IBKIE

NTT, NTT DoCoMo
Proposal for IEEE P1363.3

- HIBE (Hierarchical ID-Based Encryption)
- HIBS (Hierarchical ID-Based Signature)

- IBKIE (ID-Based Key Insulated Encryption)
HIBE


- Section 3.2 (pp.554-555)
  FullHIDE: HIDE with Chosen Ciphertext Security

Let Level, be the set of entities at level i, where Level0 = {Root PKG}. Let K be the security parameter given to the setup algorithm, and let $\mathcal{G}$ be a BDH parameter generator.

**Root Setup:** The root PKG:
1. runs $\mathcal{G}$ on input K to generate groups $G_1, G_2$ of some prime order q and an admissible pairing $\hat{e}: G_1 \times G_1 \rightarrow \mathbb{G}_T$;
2. chooses an arbitrary generator $P_0 \in G_1$;
3. picks a random $x_0 \in \mathbb{Z}/q\mathbb{Z}$ and sets $Q_0 = s_0P_0$;
4. chooses cryptographic hash functions $H_1: \{0,1\}^n \rightarrow G_1$ and $H_2: \mathbb{G}_T \rightarrow \{0,1\}^n$ for some n. The security analysis will treat $H_1$ and $H_2$ as random oracles.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $C = \mathcal{G}_1 \times \{0,1\}^n$ where t is the level of the recipient. The system parameters are $\text{params} = (G_1, G_2, \hat{e}, P_0, Q_0, H_1, H_2)$. The root PKG's secret is $s_0 \in \mathbb{Z}/q\mathbb{Z}$.

**Setup:** As in the BasicHIDE scheme, but in addition choose hash functions $H_3: \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}/q\mathbb{Z}$ and $H_4: \{0,1\}^n \rightarrow \{0,1\}^n$.

**Lower-Level Setup:** Entity $E_i \in \text{Level}_i$ picks a random $s_i \in \mathbb{Z}/q\mathbb{Z}$, which it keeps secret.

**Extraction:** Let $E_i$ be an entity in Level_i with ID-tuple $(ID_1, \ldots, ID_t)$, where $(ID_1, \ldots, ID_i)$ for $1 \leq i \leq t$ is the ID-tuple of $E_i$'s ancestor at Level_i. Set $S_{i,0}$ to be the identity element of $G_1$. Then $E_i$'s parent:
1. computes $P_i = H_1(ID_1, \ldots, ID_i) \in G_1$;
2. sets $E_i$'s secret point $S_i$ to be $S_{i-1} + s_{i-1}P_i = \sum_{j=1}^{i-1} s_{j-1}P_j$;
3. also gives $E_i$ the values of $Q_i = s_iP_0$ for $1 \leq i \leq t-1$.

**Encryption:** To encrypt $M \in \mathcal{M}$ with the ID-tuple $(ID_1, \ldots, ID_i)$, do the following:
1. compute $P_i = H_1(ID_1, \ldots, ID_i) \in G_1$ for $1 \leq i \leq t$;
2. choose a random $\sigma \in \{0,1\}^n$;
3. set $r = H_3(\sigma, M)$, and;
4. set the ciphertext to be:

$$C = \{rP_0, rP_1, \ldots, rP_t, \sigma \oplus H_2(y'), M \oplus H_4(\sigma)\}$$

where $g = \hat{e}(Q_0, P_1) \in G_2$ as before.

**Decryption:** Let $C = \{U_0, U_2, \ldots, U_t, V, W\} \in C$ be the ciphertext encrypted using the ID-tuple $(ID_1, \ldots, ID_i)$. If $(U_0, U_2, \ldots, U_t) \not\in G_1^i$, reject the ciphertext.
To decrypt $C$, $E_i$ does the following:
1. computes

$$\sigma = H_3(r, M) \cdot \frac{\hat{e}(U_0, S_i)}{\prod_{j=1}^{i-1} \hat{e}(Q_{i-1}, U_j)}$$

2. computes $W \oplus H_4(\sigma) = M$;
3. sets $r = H_3(\sigma, M)$ and tests that $(U_0, U_2, \ldots, U_t, V)$ is a BasicHIDE encryption of $M$ using $r$ and $(ID_1, \ldots, ID_i)$. If not, it rejects the ciphertext.
4. outputs $M$ as the decryption of $C$. 
Hierarchical ID-Based Signature (HIDS) Schemes

Section 4 (pp.555-557)


Root Setup: The root PKG:
1. runs $\mathcal{IG}$ on input $K$ to generate groups $G_1,G_2$ of prime order $q$ and an admissible pairing $\mathcal{e}: G_1 \times G_1 \rightarrow G_2$;
2. chooses an arbitrary generator $P_0 \in G_1$;
3. picks a random $s_0 \in \mathbb{Z}/q\mathbb{Z}$ and sets $Q_0 = s_0 P_0$;
4. chooses cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_3 : \{0,1\}^* \rightarrow G_1$. The security analysis will treat $H_1$ and $H_3$ as random oracles.

The signature space is $\mathcal{S} = G_1^{t+1}$ where $t$ is the level of the signer. The system parameters are $\text{par}_m = (G_1, G_2, \mathcal{e}, P_0, Q_0, H_1, H_3)$. The root PKG’s secret is $s_0 \in \mathbb{Z}/q\mathbb{Z}$.

Lower-Level Setup: As in BasicHIDE.

Extraction: As in BasicHIDE.

Signing: To sign $M$ with ID-tuple $(ID_1, \ldots, ID_t)$ (using the secret point $S_i = \sum_{i-1}^{\infty}s_{i-1}P_i$ and the points $Q_i = s_i P_0$ for $1 \leq i \leq t$), do the following:
1. Compute $P_M = H_3(ID_1, \ldots, ID_t, M) \in G_1$. (As suggested above, we might use a bit-prefix or some other method, instead of using a totally different hash function.)
2. Compute $\text{Sig}(\text{ID-tuple}, M) = S_t + s_t P_M$.
3. Send $\text{Sig}(\text{ID-tuple}, M)$ and $Q_t = s_t P_0$ for $1 \leq i \leq t$.

Verification: Let $[\text{Sig}, Q_1, \ldots, Q_t] \in \mathcal{S}$ be the signature for $(\text{ID-tuple}, M)$. The verifier confirms that:

$$\mathcal{e}(P_0, \text{Sig}) = \mathcal{e}(Q_0, P_1) \mathcal{e}(Q_t, P_M) \prod_{i=2}^{t} \mathcal{e}(Q_{t-1}, P_i).$$
Key Insulated IBE


- Section 5 (p.506-508)
  Efficient Construction from Bilinear Mapping

Fig. 2. KE-CCA Secure IKE from Bilinear Mapping
HIBE/ IBKIE + FO encoding

- Section 4
  Modified FO Conversion

Modified FO Conversion

Let $\Pi = \{S, X, E, D\}$ be an IBE scheme which is secure in the sense of OW-ID-CPA. We denote the new encryption scheme as $\Pi'' = \{S'', X'', E'', D''\}$. Let $l_1$ be a bit length of a plaintext of $\Pi$, $l_2$ be a bit length of a plaintext of $\Pi''$ and $\text{COIN}(k)$ be $\Pi$’s coin-flipping space.

- $S''$, the setup algorithm. It is as $S$. In addition we pick two hash functions $G : (0,1)^{l_1} \times (0,1)^{l_2} \times (0,1)^* \rightarrow \text{COIN}(k)$ and $H : (0,1)^{l_1} \rightarrow (0,1)^{l_2}$.
- $X''$, the extraction algorithm. It is as $X$.
- $E''$, the encryption algorithm. It takes system parameter $\text{params}$, public key $ID \in \{0,1\}^*$, random coin $\sigma \in \{0,1\}^{l_1}$ and a message $M \in \{0,1\}^{l_2}$. It is defined as follows:

$$E''(\text{params}, ID, \sigma, M) = E(\text{params}, ID, \sigma; G(\sigma, M, ID)) \| H(\sigma) \oplus M$$

- $D''$, the decryption algorithm. Let $C = C_1\|C_2$ be a ciphertext to decrypt. This algorithm works in the following four steps:
  1. Computes $D(\text{params}, d, C_1) = \sigma$
  2. Computes $H(\sigma) \oplus C_2 = M$
  3. Sets $r = G(\sigma, M, ID)$. Test that $E(\text{params}, ID, M; r) = C_1$. If not, outputs “reject”.
  4. Outputs $M$ as the decryption of $C$. 
Other Information

- Claimed attributes and advantages of the technique.
- Security assessment and considerations.
- Known limitations and disadvantages.

- See the original paper [1] and [2]
Patent Issue

NTT DoCoMo believes to hold granted patents and pending applications, which would be required to implement HIBE, HIBS and IBKIE.

NTT DoCoMo is prepared to grant a license on the basis of reciprocity and non-discriminatory with reasonable terms and conditions to comply with the proposed Standard.