1. Choose $b \xleftarrow{\$} \{0, 1\}$ and two random polynomials f_1, f_2 of degree 1 from $\mathbb{Z}_N[x]$, and calculate $g_1(x) = f_1(x)^2 \bmod (x^2 - w) = a_1 x + a_0$ and $g_2(x) = f_2(x)^2 \bmod (x^2 - uw) = b_1 x + b_0$. The corresponding ciphertext is

$$C_b = \begin{cases} \{a_0, a_1, N - b_0, N - b_1\}, & \text{if } b = 0; \\ \{N - a_0, N - a_1, b_0, b_1\}, & \text{otherwise.} \end{cases}$$

2. Give C_b to $\mathcal{A}_2$ —— $\mathcal{A}_2$ may issue more hash queries and extraction queries except that the query identity subset ID_2 cannot contain id^*. Finally, $\mathcal{A}_2$ returns a bit b'.

3. If $b = b'$ return 1; otherwise return 0.

We shall only analyze the success probability of $\mathcal{B}$ solving the MER_2^0 assumption in the case $w = \mathscr{H}(id^*)$ as the analyse of the case $w \neq \mathscr{H}(id^*)$ is the same as that in the proof of Proposition 1 in [25]. If $w \in \mathcal{ER}_{N,2}$, according to the fact that $uw \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}$ and Theorem 2, we conclude that C_b is a valid ciphertext for $(-1)^b$. For the same reason, if $w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}$, we conclude that C_b is a valid ciphertext for $(-1)^{1-b}$. Hence, $\mathcal{B}$ returns 1 if and only if $\mathcal{A}$ loses the game. Let ϵ be the probability that $\mathcal{A}$ can break the $\mathsf{IND\text{-}ID\text{-}CPA}$ security of Π_2, thus we have

$$\begin{aligned} &\Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{ER}_{N,2}\right] = \\ &\qquad \Pr[w = \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{ER}_{N,2} \wedge w = \mathscr{H}(id^*)\right] + \\ &\qquad\qquad \Pr[w \neq \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{ER}_{N,2} \wedge w \neq \mathscr{H}(id^*)\right] \end{aligned}$$

$$\begin{aligned} &\Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}\right] = \\ &\qquad \Pr[w = \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2} \wedge w = \mathscr{H}(id^*)\right] + \\ &\qquad\qquad \Pr[w \neq \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2} \wedge w \neq \mathscr{H}(id^*)\right] \end{aligned}$$

$$\begin{aligned} \mathsf{Adv}_{\mathcal{B},\mathrm{RSAgen}}^{\mathsf{MER}_2^0}(\lambda) &= \left|\Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{ER}_{N,2}\right] - \Pr\left[\mathcal{B}(N, w, u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}\right]\right| = \\ &\left|\frac{\epsilon}{q_{\mathscr{H}}} + \left(1 - \frac{1}{q_{\mathscr{H}}}\right) \cdot \frac{1}{2} - \left(\frac{1-\epsilon}{q_{\mathscr{H}}} + \frac{1 - \frac{1}{q_{\mathscr{H}}}}{2}\right)\right| = \frac{2}{q_{\mathscr{H}}} \cdot \mathsf{Adv}_{\mathcal{A},\Pi_2}^{\mathsf{IND\text{-}ID\text{-}CPA}}(\lambda) \end{aligned}$$

■

Construction for Prime Number e Inspired by the approach used in CM scheme to avoid such a hash in BLS scheme, our IBE scheme Π_e for a prime e is defined as follows:

$\mathsf{Setup}(1^\lambda)$ Given a security parameter λ, Setup generates an RSA modulus $N = pq$ a product of two distinct large primes p and q, and selects a prime number e such that $e \mid p - 1$, $e \mid q - 1$ and $\gcd(\frac{p+q-2}{e}, e) = 1$. Setup also selects an element $u \in \mathcal{J}_{N,e}^1 \setminus \mathcal{ER}_{N,e}$. The settings of μ is the same as in BLS scheme. The public parameter is $\mathsf{mpk} = \{N, e, u, \mu, \mathscr{J}_{N,e}(\mu), \mathscr{H}\}$ where $\mathscr{H}$ is a publicly available cryptographic hash function mapping an arbitrary binary string to $\mathcal{J}_{N,e}^1$. The master secret key is $\mathsf{msk} = \{p, q\}$.

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, id)$ Using mpk and msk, KeyGen sets $R_{id} = \mathscr{H}(id)$, then computes $\left(\frac{R_{id}}{\mathfrak{p}_1}\right)_e = \zeta_e^{j_1}$ and $r_{id} = (R_{id} u^{-j_1 j_2^{-1} \bmod e})^{\frac{1}{e}} \bmod N$ where $\left(\frac{u}{\mathfrak{p}_1}\right)_e = \zeta_e^{j_2}$. Finally, KeyGen returns

$$\mathsf{sk}_{id} = \left\{o = -j_1 j_2^{-1} \bmod e,\ r_{id}\right\}$$

as user's private key.

$\mathsf{Enc}\,(\mathsf{mpk}, id, m)$ To encrypt a message $m \in \mathbb{Z}_e$ for a user with identity id, Enc first derives the hash value $R_{id} = \mathscr{H}\,(id)$. Then, it generates $t = \mu^k$ where $k \xleftarrow{\$} \mathbb{Z}_e$. We define the sub-algorithm $\mathcal{E}$ which takes as inputs a prime number $\mathcal{P}$ and two integers $\mathcal{N}$ and k as Algorithm 1.

Algorithm 1 $\mathcal{E}$

Input: a prime number $\mathcal{P}$, two integers $\mathcal{N}$ and k
Output: a polynomial

1: Generate a uniform random polynomial $f(x) \xleftarrow{\$} \mathbb{Z}_N^*[x]$ of degree $\mathcal{P} - 1$
2: Compute $g(x) \leftarrow f(x)^{\mathcal{P}} \bmod x^{\mathcal{P}} - \mathcal{N}$
3: Output the polynomial $c(x) = \frac{g(x)}{\mu^k \bmod \mathcal{P}}$

The returned ciphertext is

$$C = \begin{Bmatrix} \left\{ \mathcal{E}\left(e, u^i R_{id}, k\right) \,\middle|\, 0 \le i < e \right\} \\ \left(m + \mathscr{J}_{N,e}\left(t\right)\right) \bmod e \end{Bmatrix}$$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{id}, C)$ When a user with $\mathsf{sk}_{id} = \{o,\, r_{id}\}$ receives a ciphertext set C, it parses C as

$$C = \{c_0(x), \ldots, c_{e-1}(x), c\}\,.$$

Dec recovers the plaintext m as

$$m = \left(\mathscr{J}_{N,e}\left(c_o(r_{id})\right) + c\right) \bmod e$$

Remark 3. The condition $\gcd(\frac{p+q-2}{e}, e) = 1$ ensures that $\mathscr{J}_{N,e}(\mu)$ is relatively prime to e through the proof of Proposition 1. In the Enc algorithm, computing $\mathscr{J}_{N,e}\left(t\right) = k\mathscr{J}_{N,e}(\mu) \bmod e$ can be very convenient. In the KeyGen algorithm, the secret key can be successfully derived since $\left(\frac{x}{\mathsf{p}_1}\right)_e = \left(\frac{x}{\mathsf{q}_1}\right)_e = 1$ where $x = u^o R_{id} \bmod N$. According to Theorem 1, there must exist $y \in \mathbb{Z}_p^*$ and $z \in \mathbb{Z}_q^*$ for which $y^e \equiv x \bmod p$ and $z^e \equiv x \bmod q$.

<u>*Correctness*</u> *Correctness* can be verified directly as follows.

$$\begin{aligned} \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{id}, (\mathsf{Enc}(id, m))) &\equiv \mathscr{J}_{N,e}\left(c_o(r_{id})\right) + m + \mathscr{J}_{N,e}(\mu^k) \\ &\equiv \mathscr{J}_{N,e}\left(\frac{1}{\mu^k}\right) + m + \mathscr{J}_{N,e}(\mu^k) \quad (\text{ because } r_{id}^e \equiv u^o R_{id} \bmod N) \\ &\equiv m \pmod{e} \end{aligned}$$

Theorem 4. *Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary against the* IND-ID-CPA *security of our scheme Π_e, making at most $q_{\mathscr{H}}$ queries to the random oracle $\mathscr{H}$ and a single query to the* Challenge phase*. Then, there exists an adversary $\mathcal{B}$ against the* MER_e^1 *assumption such that*

$$\mathsf{Adv}_{\mathcal{A},\Pi_e}^{\mathsf{IND\text{-}ID\text{-}CPA}}(\lambda) = \frac{q_{\mathscr{H}}}{2} \cdot \mathsf{Adv}_{\mathcal{B},RSAgen}^{\mathsf{MER}_e^1}(\lambda)$$

Proof. We have already proved that this theorem holds when $e = 2$. For a general prime e, we need to modify what will the challenger $\mathcal{B}$ do after receiving two different plaintexts m_0 and m_1, especially the process 1 ($\mathscr{H}(id^*) = w \in \mathcal{J}_{N,e}^1$) in previous proof as:

1. Choose $b \xleftarrow{\$} \{0,1\}$ and $k \xleftarrow{\$} \mathbb{Z}_e$. Let $j = \mathscr{J}_{N,e}(\mu)^{-1} \bmod e$. The corresponding ciphertext is

$$C_b = \begin{cases} \left\{\begin{array}{c} \mathcal{E}\left(e, w, k\right) \\ \mathcal{E}\left(e, u^1 w, k + (m_0 - m_1) j\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k + (m_0 - m_1) j\right) \\ \left(m_0 + \mathscr{J}_{N,e}\left(\mu^k\right)\right) \bmod e \end{array}\right\} & \text{if } b = 0; \\ \\ \left\{\begin{array}{c} \mathcal{E}\left(e, w, k\right) \\ \mathcal{E}\left(e, u^1 w, k + (m_1 - m_0) j\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k + (m_1 - m_0) j\right) \\ \left(m_1 + \mathscr{J}_{N,e}\left(\mu^k\right)\right) \bmod e \end{array}\right\} & \text{otherwise.} \end{cases}$$

If $w \in \mathcal{ER}_{N,e}$, then $\left(\frac{u^i w}{\mathfrak{p}_1}\right)_e$ and $\left(\frac{u^i w}{\mathfrak{q}_1}\right)_e$ are both primitive for all $0 < i < e$. From Theorem 2, C_b is computationally equivalent to C'_b where

$$C'_b = \begin{cases} \left\{\begin{array}{c} \mathcal{E}\left(e, w, k\right) \\ \mathcal{E}\left(e, u^1 w, k\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k\right) \\ \left(m_0 + \mathscr{J}_{N,e}\left(\mu^k\right)\right) \bmod e \end{array}\right\} & \text{if } b = 0; \\ \\ \left\{\begin{array}{c} \mathcal{E}\left(e, w, k\right) \\ \mathcal{E}\left(e, u^1 w, k\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k\right) \\ \left(m_1 + \mathscr{J}_{N,e}\left(\mu^k\right)\right) \bmod e \end{array}\right\} & \text{otherwise.} \end{cases}$$

Thus, C_b is a valid ciphertext for m_b. If $w \in \mathcal{J}^1_{N,e} \setminus \mathcal{ER}_{N,e}$, for the same reason, C_b is computationally equivalent to $\overline{C_b}$ where

$$\overline{C_b} = \begin{cases} \left\{\begin{array}{c} \mathcal{E}\left(e, w, k + (m_0 - m_1) j\right) \\ \mathcal{E}\left(e, u^1 w, k + (m_0 - m_1) j\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k + (m_0 - m_1) j\right) \\ \left(m_1 + \mathscr{J}_{N,e}\left(\mu^{k + (m_0 - m_1) j}\right)\right) \bmod e \end{array}\right\} & \text{if } b = 0; \\ \\ \left\{\begin{array}{c} \mathcal{E}\left(e, w, k + (m_1 - m_0) j\right) \\ \mathcal{E}\left(e, u^1 w, k + (m_1 - m_0) j\right) \\ \vdots \\ \mathcal{E}\left(e, u^{e-1} w, k + (m_1 - m_0) j\right) \\ \left(m_0 + \mathscr{J}_{N,e}\left(\mu^{k + (m_1 - m_0) j}\right)\right) \bmod e \end{array}\right\} & \text{otherwise.} \end{cases}$$

In this case, C_b is a valid ciphertext for m_{1-b}.

The reader can easily fill in the remaining details of the proof from the proof of Theorem 3. ■