:

Algorithm 1 Prover : P_{OE} on input (x, w)

// Create t.c proofs and hash each response
for $i = 1$ **to** t **do**
    $com_i \leftarrow P^1_\Sigma(x, w)$
    for $j = 1$ **to** c **do**
        $ch_{i,j} \leftarrow_R N_{ch} \setminus \{ch_{i,1}, \cdots, ch_{i,j-1}\}$
        $resp_{i,j} \leftarrow P^2_\Sigma(x, w, com, ch_{i,j})$
        $h_{i,j} \leftarrow G(resp_{i,j})$
// Get challenge by hashing
$J_1 \parallel \cdots \parallel j_t \leftarrow H(x(com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j})$ ▷ Get challenge by hashing
// return proof
return $\pi \leftarrow ((com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j}, (resp_{i,J_i})_i)$ ▷ return proof

Algorithm 2 Verifier : V_{OE} on input (x, π) where

$\pi = ((com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j}, (resp_{i,J_i})_i)$

// Compute the challenge hash

for $i = 1$ **to** t **do**

    check $ch_{i,1}, \cdots ch_{i,m} pairwise distinct$

    check $h_{i,J_i} = G(resp_i)$

    check $V_\Sigma(x, com_i, ch_{i,J_i}, resp_i) = 1$

if all checks succeed **then return** 1

Algorithm 3 $KeyGen(\lambda)$

Pick a random point S of order $\ell_A^{e_A}$

Compute the isogeny $\phi : E \to E/\langle S \rangle$

$pk \leftarrow (E/\langle S \rangle, \phi(P_B), \phi(Q_B))$

$sk \leftarrow S$

return (pk, sk)

Algorithm 4 $Sign(sk, m)$

for i=1 **to** 2λ **do**
    Pick a random point R of order $\ell_B^{e_B}$
    Compute the isogeny $\psi : E \to E/\langle R \rangle$
    Compute either $\phi' : E/\langle R \rangle \to E/\langle R, S \rangle$ *or* $\psi' : E/\langle S \rangle \to E/\langle R, S \rangle$
    $(E_1, E_2) \leftarrow (E/\langle R \rangle, E/\langle R, S \rangle)$
    $com_i \leftarrow (E_1, E_2)$
    $ch_{i,0} \leftarrow_R \{0, 1\}$
    $(resp_{i,0}, resp_{i,1}) \leftarrow ((R, \phi(R)), \psi(S))$
    if $ch_{i,0} = 1$ **then**
        swap $(resp_{i,0}, resp_{i,1})$
    $h_{i,j} \leftarrow G(resp_{i,j})$
$J_1 \parallel \cdots \parallel J_{2\lambda} \leftarrow H(pk, m, (com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j})$
return $\sigma \leftarrow ((com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j}, (resp_{i,J_i})_i)$

Algorithm 5 $Sign(sk, m)$

$J_1 \parallel \cdots \parallel J_{2\lambda} \leftarrow H(pk, m, (com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j})$

for i=1 **to** 2λ **do**

    check $h_{i,J_i} = G(resp_{i,J_i})$

    if $ch_{i,J_i} = 0$ **then**

        Parse $(R, \phi(R)) \leftarrow resp_{i,J_i}$

        check $R, \phi(R)$ have order $\ell_B^{e_B}$

        check R generates the kernel of the isogeny $E \leftarrow E_1$

        check $\phi(R)$ generates the kernel of the isogeny $E/\langle S \rangle \rightarrow E_2$

    else if **then**

        Parse $\psi(S) \rightarrow resp_{i,J_i}$

        check $\psi(S)$ has order $\ell_A^{e_A}$

        check $\psi(S)$ generates the kernel of the isogeny $E_1 \rightarrow E_2$

if all checks successd **then**

    return 1