Attack

Notations For the following, $z|t = E(x|y) = E_3(E_1(x) \oplus f(E_1(x) \oplus E_2(y)))|E_4(E_2(y) \oplus f(E_1(x) \oplus E_2(y)))$, n is the size of the total input and k is the size of keys in E_1, E_2, E_3, E_4, f

limitation of the security of the construction: The following procedure takes $\tilde{O}(2^{max(k/2,n/6)})$ computations and recovers the key of E_2, the same can be done for E_1, E_3 or E_4:

- Choose two inputs x_1 and x_2 for the input that goes into E_1
- Search collisions on the left part of the outputs of encryptions of messages $x_1|y$ and $x_2|y'$. (repeat the process n times) With the construction, we get n superposition of the elements of the set $\{(y, y')/f(E_1(x_1) \oplus E_2(y)) \oplus f(E_1(x_1) \oplus E_2(y')) = E_1(x_1) \oplus E_1(x_2)\}$
- Search the key for E_2 with the following oracle:
  - reorder the superposition with $y \leftarrow E_2^{-1}(y)$. The set becomes (with the right guess) $\{(y, y')/f(E_1(x_1) \oplus y) \oplus f(E_1(x_1) \oplus y') = E_1(x_1) \oplus E_1(x_2)\}$ The set has an involution $(y, y') \mapsto (y' \oplus E_1(x_1) \oplus E_1(x_2), y' \oplus E_1(x_1) \oplus E_1(x_2))$.
  - apply $(y, y') \mapsto (y, y' \oplus y$(noted as A)). The set now has an involution $(y, A) \mapsto (y \oplus A \oplus E_1(x_1) \oplus E_1(x_2), A)$.
  - apply an Hadamard gate on the first variable, the superposition now contains elements (m, A) such that $m.(E_1(x_1) \oplus E_1(x_2)) = m.A$ if we guessed right and something random if not.
  - apply the steps above to others couples of variables and compute $E_1(x_1) \oplus E_1(x_2)$ many times
  - return 1 if we get the same value (right guess with high probability),0 if we don't (wrong guess)
  - uncompute the steps above