Combining Function

Let E_k be a symmetric encryption with a secret key K.

$$C_{k,v}(y_1, \cdots, y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus \cdots \oplus E_k(y_1 + v) \cdots))$$

Then, i) $C_{k,v}$ is 1-1 mapping from y_s to z for $1 \le s \le r$ and fixed y_i, $i \neq s$.

ii) For $1 \le s \le r$ and y_i, $i \neq s$,

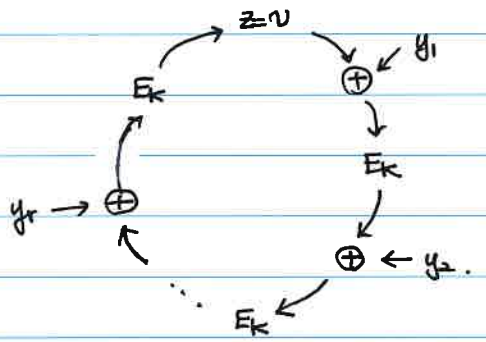
it is possible to efficiently find y_s s.t. $C_{k,v}(y_1, y_2, \cdots, y_r) = z$.

iii) Given k, z, and v,

it is hard to solve $C_{k,v}(g_1(x_1), \cdots, g_r(x_r)) = z$ for $x_1, \cdots, x_r$

if g_i's are one-way function.

If $z = C_{k,v}(y_1, y_2, \cdots, y_r) = v$,



RSA. Encrypt(x) for P_i

Define $g_i(x) = x^{e_i} \bmod n_i$.

one can easily obtain m if he/she has d_i s.t. $e_i d_i \equiv 1 \bmod n_i$.

However, if he/she does not have such d_i, it is hard to obtain m.