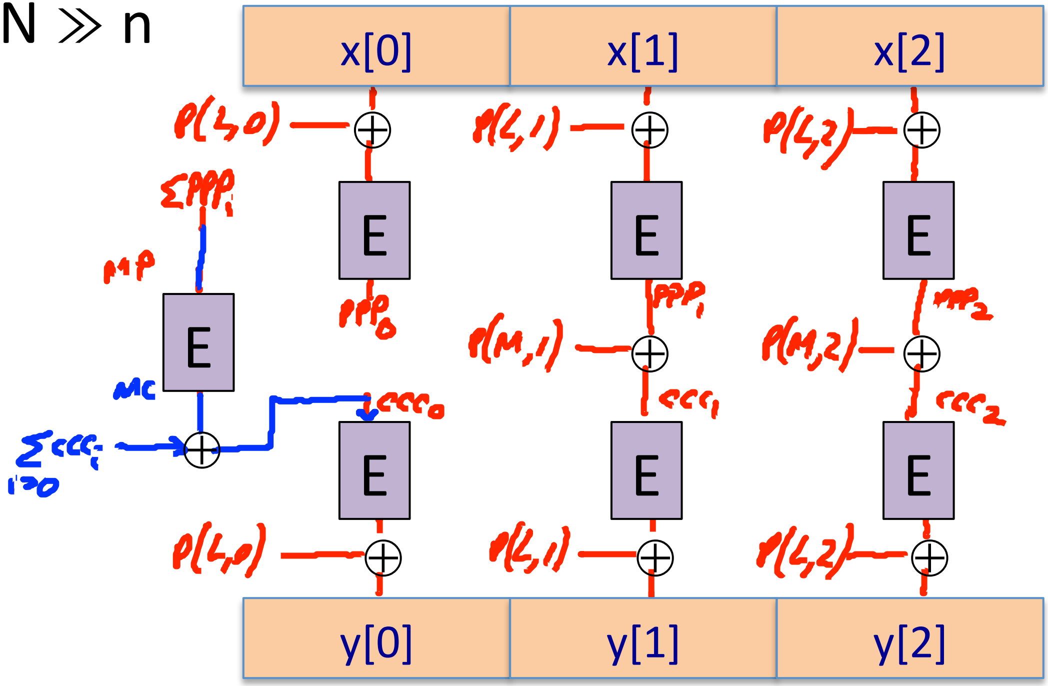
Let (E, D) be a secure PRP. E: K × $\{0,1\}^n \longrightarrow \{0,1\}^n$

EME: a PRP on $\{0,1\}^N$ for $N \gg n$

Key = (K, L)

$M \leftarrow MP \oplus MC$



Performance:

- can be 2x slower then SIV