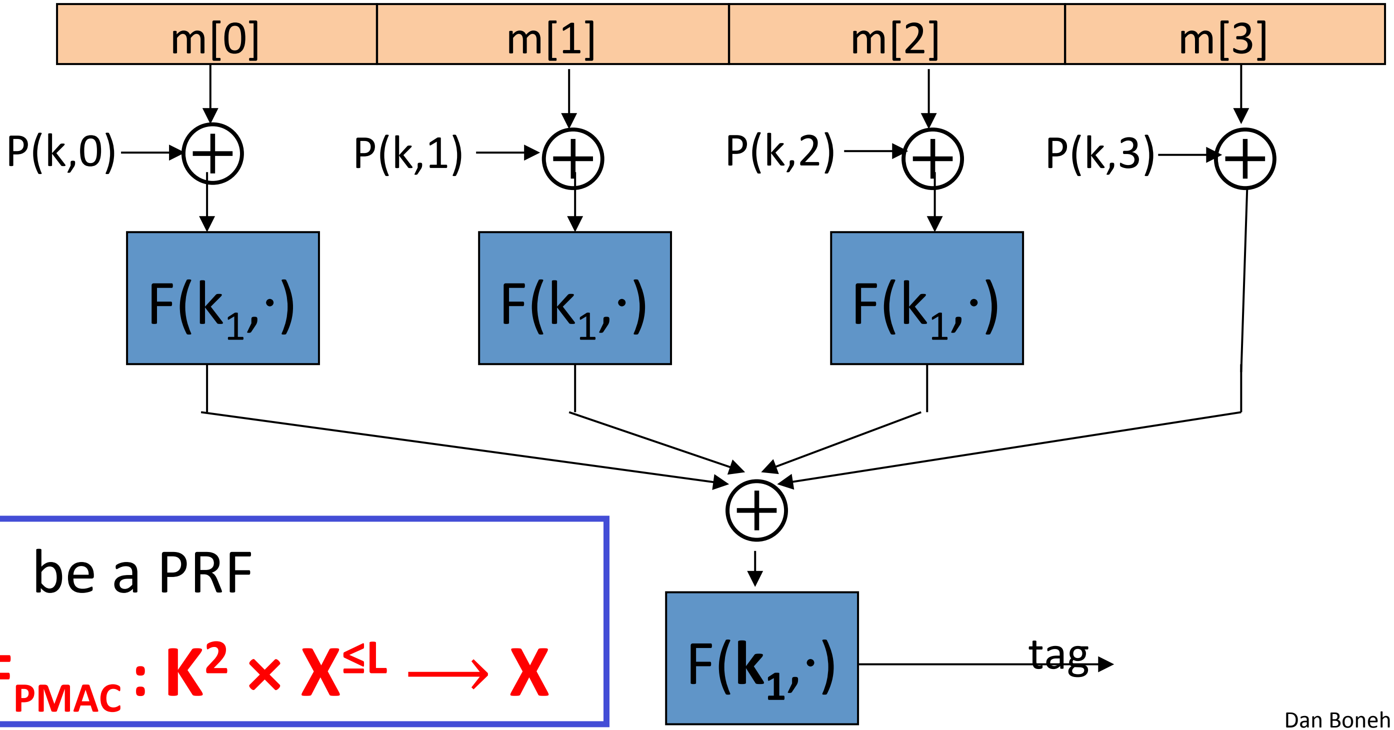
P(k, i): an easy to compute function

key = (k, k_1)

Padding similar to CMAC



Let **$F: K \times X \longrightarrow X$** be a PRF

Define new PRF **$F_{PMAC} : K^2 \times X^{\leq L} \longrightarrow X$**