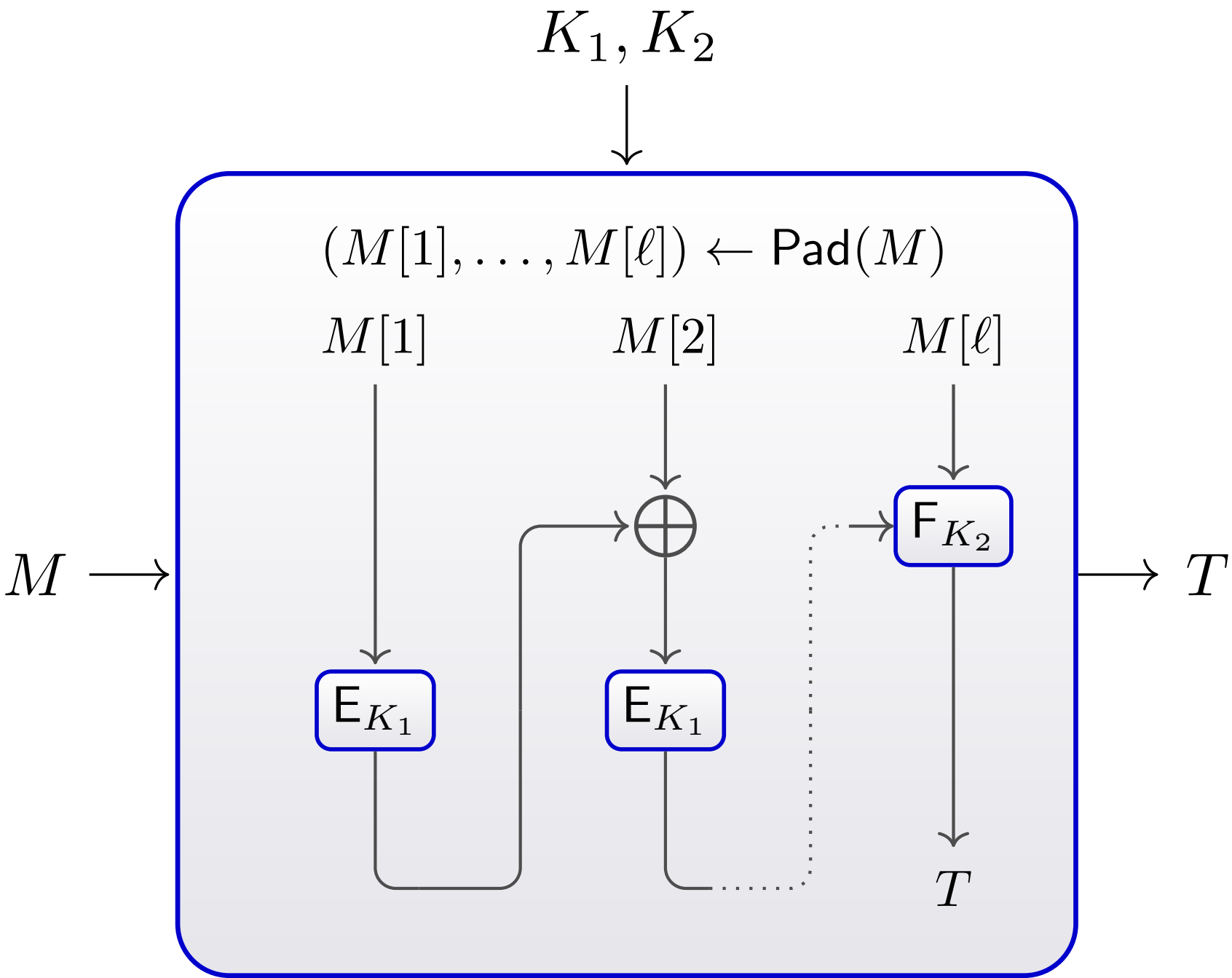
K_1, K_2
$(M[1], \ldots, M[\ell]) \leftarrow \mathsf{Pad}(M)$
$M[1]$
$M[2]$
$M[\ell]$
M
E_{K_1}
E_{K_1}
F_{K_2}
T
T