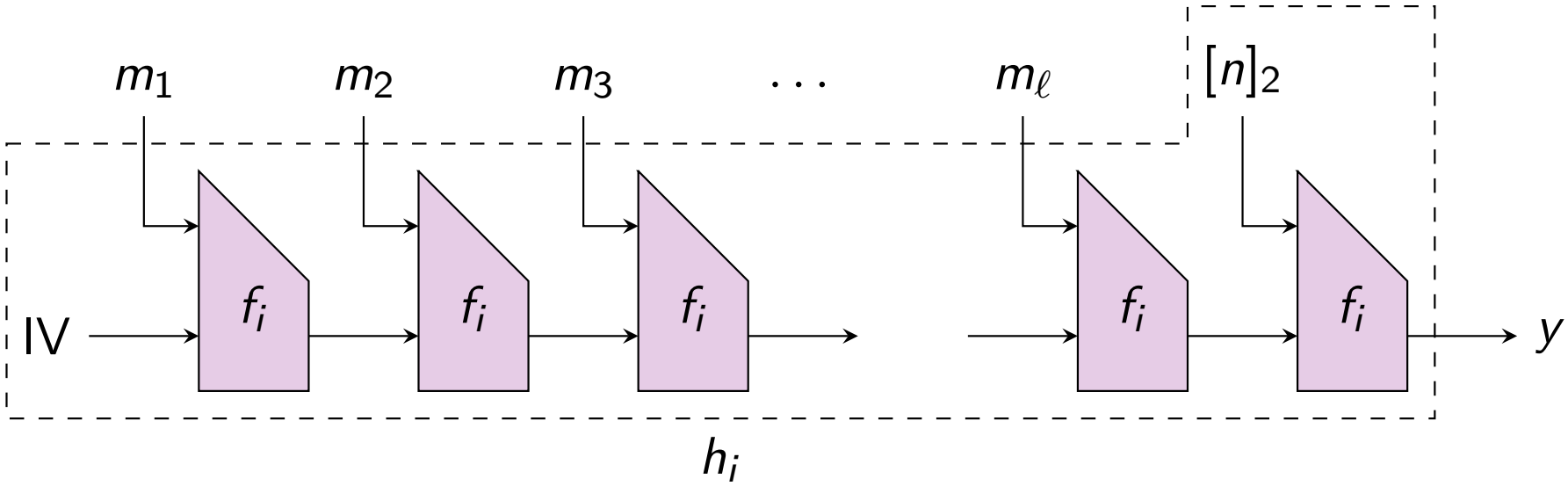
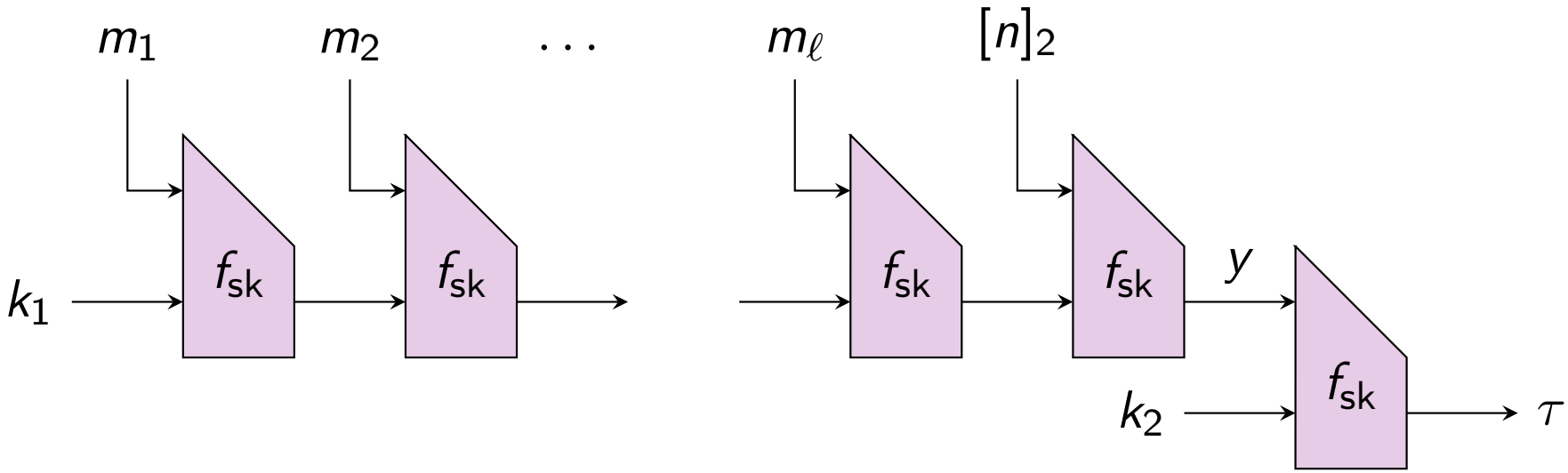
Lecture 27: Merkle-Damgård CRHF Construction & NMAC, HMAC Constructions

Merkle-Damgård Transform

Suppose we have $m \in \{0,1\}^n$ and we interpret it as $(m_1, m_2, \ldots, m_\ell)$, where $\ell = \lceil n/B \rceil$



NMAC Construction



HMAC Construction