- We say that a *fruit*, $f = (h_{-1}; h'; \eta, \mathsf{digest}; \mathsf{m}; h)$, *is valid* iff $H(h_{-1}; h'; \eta; \mathsf{digest}; \mathsf{m}) = h$ and $[h]_{-\kappa:} < D_{p_f}$ where $[h]_{-\kappa:}$ denotes the last $\kappa$ bits of $h$; we call $h'$ the pointer of $f$. *$F$ is a valid fruit-set* if either $F = \emptyset$ or $F$ is a set of valid fruits.