

- We say that a *block*, $b = (h_{-1}; h'; \eta; \text{digest}; m; h), F$, is *valid* iff $\text{digest} = d(F)$, F is a valid fruit-set, $H(h_{-1}; h'; \eta, d(F); m) = h$ and $[h]_{:\kappa} < D_{p_1}$ where $[h]_{:\kappa}$ denotes the first κ bits of h ; we call h the *reference* of b .