Proh 45 v = [g"y modp] modq = r = [y modp] modq [g"modp)(y"modp)] modp modq E[(p+1) mod p] mod p (y mod p) } mod p mod q [y mod p] mod q = [y mod p] mod q $v_2 = r(s^{-1}m \circ dq) m \circ dq$ S = rz-1 modq → V2 = Z r (5-1 modg) modg r ([rz-1 modg] modg) modg r ((rz-1) -1 madq) madq r (r-1 z mod q) mod q protzmedq = 2 This is true when N = hash disest size which it so for N=120 and SHA-1