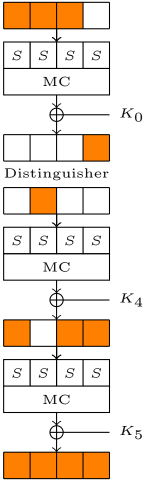
Backward differential(similar to forward differential) and forward determination(similar to backward determination)

Values of $K_{-1}[0,1,2]$ are also enough to construct a plaintext structure which will be a δ-set for the distinguisher with $U_0[3]$ active, where K_{-1} is the white key.

Values of $P(U_0[0,1,2])$ are enough to construct a plaintext structure which will be a δ-set for the distinguisher with $U_0[3]$ active.



$Input_{-1}\_typeX = \_X(U_{-1}) = [U_{-1}[0]\_typeX, U_{-1}[1]\_typeX, U_{-1}[2]\_typeX, U_{-1}[3]\_typeX] = [1,1,1,0]$

$\uparrow$ SB **MITMConstraints.equalConstraints($InputMC_{-1}\_typeX$, $Input_{-1}\_typeX$)**

$InputMC_{-1}\_typeX = \_X(V_{-1}) = [V_{-1}[0]\_typeX, V_{-1}[1]\_typeX, V_{-1}[2]\_typeX, V_{-1}[3]\_typeX] = [1,1,1,0]$

MC $\uparrow$ AK **MITMConstraints.ForwardDiff_LinearLayerr(MC^{-1},$Input_0\_typeX$,$InputMC_{-1}\_typeX$)**

$Input_0\_typeX = \_X(U_0) = [U_0[0]\_typeX, U_0[1]\_typeX, U_0[2]\_typeX, U_0[3]\_typeX] = [0,0,0,1]$

$Input_3\_typeY = \_Y(U_3) = [U_3[0]\_typeY, U_3[1]\_typeY, U_3[2]\_typeY, U_3[3]\_typeY] = [0,1,0,0]$

$\downarrow$ SB **MITMConstraints.equalConstraints($Input_3\_typeY$, $InputMC_3\_typeY$)**

$InputMC_3\_typeY = \_Y(V_3) = [V_3[0]\_typeY, V_3[1]\_typeY, V_3[2]\_typeY, V_3[3]\_typeY] = [0,1,0,0]$

MC $\downarrow$ AK **MITMConstraints.BackwardDet_LinearLayer(MC^{-1},$Input_4\_typeY$,$InputMC_3\_typeY$)**

$Input_4\_typeY = \_Y(U_4) = [U_4[0]\_typeY, U_4[1]\_typeY, U_3[2]\_typeY, U_3[3]\_typeY] = [1,0,1,1]$

$\downarrow$ SB **MITMConstraints.equalConstraints($Input_4\_typeY$, $InputMC_4\_typeY$)**

$InputMC_4\_typeY = \_Y(V_4) = [V_4[0]\_typeY, V_4[1]\_typeY, V_4[2]\_typeY, V_4[3]\_typeY] = [1,0,1,1]$

MC $\downarrow$ AK **MITMConstraints.BackwardDet_LinearLayer(MC^{-1},$Input_5\_typeY$,$InputMC_4\_typeY$)**

$Input_5\_typeY = \_Y(U_5) = [U_5[0]\_typeY, U_5[1]\_typeY, U_5[2]\_typeY, U_5[3]\_typeY] = [1,1,1,1]$

Values of $P(U_4[0,2,3], U_3[1])$ are enough to compute the difference of $U_3[1]$ from ciphertext.

Values of $MC^{-1}(K_5)[0,2,3])$, $MC^{-1}(K_4)[1]$are enough to compute the difference of $U_3[1]$ from ciphertext.