```
Entry
          = v0
          := v1
          := 0
phi_mul
          := 0
exitcond := (i == 32)
          := i + 1
next_mul := phi_mul + 0x9e3779b9
next_reg := next_mul
          = v1_1 << 4
                                                                      := i 1
tmp
         := tmp + k0_read
                                                           phi_mul
                                                                    := next_mul
tmp1
        = v1_1 >> 5
                                                           exitcond := ( i == 32)
tmp2
                                                                      := i + 1
        := tmp2 + k1_read
tmp3
                                                           next_mul := phi_mul + 0x9e3779b9
          := v1_1 + next_reg
tmp4
next_reg2 := next_reg
                                                           next_reg := next_mul
          := tmp3 xor tmp4
tmp5
          := tmp5 xor tmp1
tmp6
v0_2
tmp7
         := tmp6 + v0_1
        = v0_2 << 4
                                                                                                                                    := i_1
                                                                      = v1_1 << 4
        := tmp7 + k2\_read
tmp8
                                                                                                                         phi_mul := next_mul
                                                                     := tmp + k0_read
         = v0_2 >> 5
tmp9
                                                                                                                         exitcond := ( i == 32)
                                                                     = v1_1 >> 5
         := tmp9 + k3_read
tmp10
                                                                                                                                    := i + 1
                                                                     := tmp2 + k1_read
                                                           tmp3
          := v0_2 + next_reg2
tmp11
                                                                                                                         If exitcond goto Ppost else goto NextStep
                                                                      := v1_1 + next_reg
          := tmp11 xor tmp8
tmp12
                                                                                                                         next_mul := phi_mul + 0x9e3779b9
                                                           next_reg2 := next_reg
          := tmp12 + tmp10
tmp13
                                                                                                                         next_reg := next_mul
          := tmp13 + v1_1
                                                                                                                         Goto Beginning of Ploop
          = v0_2
          = v1_2
                                                                                                                                    := tmp3 xor tmp4
                                                                                                                         tmp5
                                                                                                                                    := tmp5 xor tmp1
                                                                                                                         tmp6
                                                                                                                                   = tmp6 + v0_1
= v0_2 << 4
                                                                                                                         v0_2
                                                                                                                         tmp7
                                                                                                                                   := tmp7 + k2\_read
                                                                                                                         tmp8
                                                                                                                                   = v0_2 >> 5
                                                                                                                         tmp9
                                                                                                                                   := tmp9 + k3_read
                                                                                                                         tmp10
                                                                                                                                   := v0_2 + next_reg2
                                                                                                                         tmp11
                                                                                                                                   := tmp11 xor tmp8
                                                                                                                         tmp12
                                                                                                                         tmp13
                                                                                                                                   := tmp12 + tmp10
                                                                                                                         v1_2
v0_1
                                                                                                                                   := tmp13 + v1_1
                                                                                                                                    = v0_2
                                                                                                                                    = v1_2
                                                                                                                                               Exit
```