Entry

```
v0_1       := v0
v1_1       := v1
i          := 0
phi_mul    := 0
exitcond   := ( i == 32)
i_1        := i + 1
next_mul   := phi_mul + 0x9e3779b9
next_reg   := next_mul
```

```
tmp        := v1_1 << 4
tmp1       := tmp + k0_read
tmp2       := v1_1 >> 5
tmp3       := tmp2 + k1_read
tmp4       := v1_1 + next_reg
next_reg2  := next_reg
```

```
i          := i_1
phi_mul    := next_mul
exitcond   := ( i == 32)
i_1        := i + 1
next_mul   := phi_mul + 0x9e3779b9
next_reg   := next_mul
```

P_{pre}

```
tmp5       := tmp3 xor tmp4
tmp6       := tmp5 xor tmp1
v0_2       := tmp6 + v0_1
tmp7       := v0_2 << 4
tmp8       := tmp7 + k2_read
tmp9       := v0_2 >> 5
tmp10      := tmp9 + k3_read
tmp11      := v0_2 + next_reg2
tmp12      := tmp11 xor tmp8
tmp13      := tmp12 + tmp10
v1_2       := tmp13 + v1_1
v0_1       := v0_2
v1_1       := v1_2
```

```
tmp        := v1_1 << 4
tmp1       := tmp + k0_read
tmp2       := v1_1 >> 5
tmp3       := tmp2 + k1_read
tmp4       := v1_1 + next_reg
next_reg2  := next_reg
```

```
i          := i_1
phi_mul    := next_mul
exitcond   := ( i == 32)
i_1        := i + 1
If exitcond goto Ppost else goto NextStep
next_mul   := phi_mul + 0x9e3779b9
next_reg   := next_mul
Goto Beginning of Ploop
```

P_{loop}

```
tmp5       := tmp3 xor tmp4
tmp6       := tmp5 xor tmp1
v0_2       := tmp6 + v0_1
tmp7       := v0_2 << 4
tmp8       := tmp7 + k2_read
tmp9       := v0_2 >> 5
tmp10      := tmp9 + k3_read
tmp11      := v0_2 + next_reg2
tmp12      := tmp11 xor tmp8
tmp13      := tmp12 + tmp10
v1_2       := tmp13 + v1_1
v0_1       := v0_2
v1_1       := v1_2
```

P_{post}

Exit