HIGHT Algorithm Specification

2009.07

1. HIGHT

The HIGHT algorithm is a symmetric block cipher that can process data blocks of 64 bits, using a cipher key with length of 128 bits.

2. HIGHT encryption

The encryption operation is as shown in Figure 1. The transformation of a 64-bit block P into a 64-bit block C is defined as follows:

(1) $P = P_7 \,//\, P_6 \,//\, P_5 \,//\, P_4 \,//\, P_3 \,//\, P_2 \,//\, P_1 \,//\, P_0$ (P_i are plaintext bytes)

(2) $X_{0,0} = P_0 \boxplus WK_0$, $X_{0,1} = P_1$,

$X_{0,2} = P_2 \oplus WK_1$, $X_{0,3} = P_3$,

$X_{0,4} = P_4 \boxplus WK_2$, $X_{0,5} = P_5$,

$X_{0,6} = P_6 \oplus WK_3$, $X_{0,7} = P_7$.

(3) for i = 0 to 30:

$$X_{i+1,0} = X_{i,7} \oplus (F_0(X_{i,6}) \boxplus SK_{4i+3}), \quad X_{i+1,1} = X_{i,0},$$

$$X_{i+1,2} = X_{i,1} \boxplus (F_1(X_{i,0}) \oplus SK_{4i}), \quad X_{i+1,3} = X_{i,2},$$

$$X_{i+1,4} = X_{i,3} \oplus (F_0(X_{i,2}) \boxplus SK_{4i+1}), \quad X_{i+1,5} = X_{i,4},$$

$$X_{i+1,6} = X_{i,5} \boxplus (F_1(X_{i,4}) \oplus SK_{4i+2}), \quad X_{i+1,7} = X_{i,6}.$$

for i = 31:

$$X_{i+1,0} = X_{i,0}, \quad X_{i+1,1} = X_{i,1} \boxplus (F_1(X_{i,0}) \oplus SK_{124}),$$

$$X_{i+1,2} = X_{i,2}, \quad X_{i+1,3} = X_{i,3} \oplus (F_0(X_{i,2}) \boxplus SK_{125}),$$

$$X_{i+1,4} = X_{i,4}, \quad X_{i+1,5} = X_{i,5} \boxplus (F_1(X_{i,4}) \oplus SK_{126}),$$

$$X_{i+1,6} = X_{i,6}, \quad X_{i+1,7} = X_{i,7} \oplus (F_0(X_{i,6}) \boxplus SK_{127}).$$

(4) $C_0 = X_{32,0} \boxplus WK_4$, $C_1 = X_{32,1}$,

$C_2 = X_{32,2} \oplus WK_5$, $C_3 = X_{32,3}$,

$C_4 = X_{32,4} \boxplus WK_6$, $C_5 = X_{32,5}$,

$C_6 = X_{32,6} \oplus WK_7$, $C_7 = X_{32,7}$.

(5) $C = C_7 \,//\, C_6 \,//\, C_5 \,//\, C_4 \,//\, C_3 \,//\, C_2 \,//\, C_1 \,//\, C_0$ (C_i are ciphertext bytes)

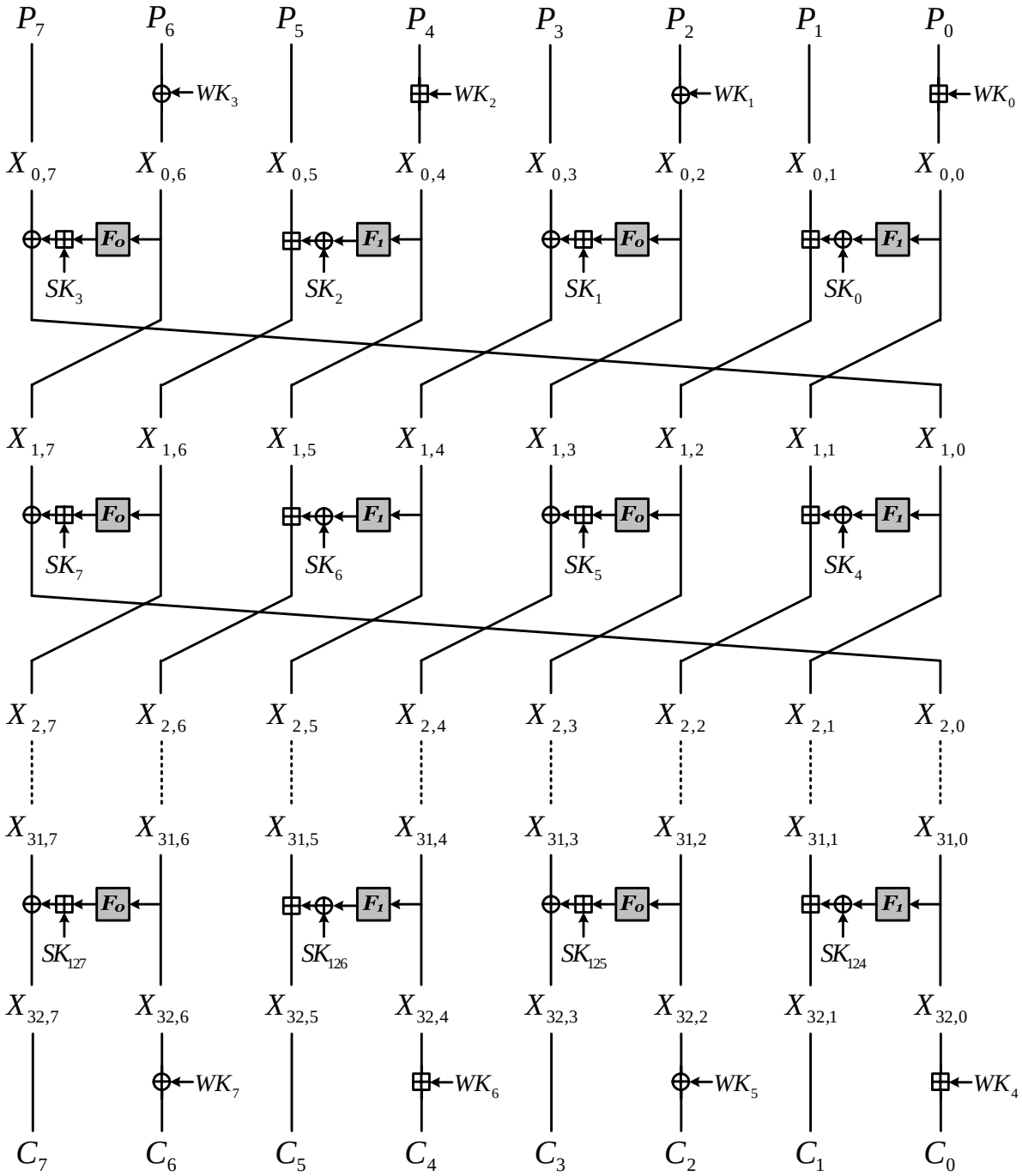

Figure 1. Encryption procedure of HIGHT

3. HIGHT decryption

The decryption operation is identical in operation to encryption apart from the following two modifications.

(1) All ⊞ operations are replaced by ⊟ operations except for the ⊞ operations connecting SK_i and outputs of F_0.

(2) The order in which the keys WK_i and SK_i are applied is reversed.

4. HIGHT functions

4.1 The functions F_0 and F_1

The HIGHT algorithm uses two functions, namely, F_0 and F_1 which are now defined.

4.2 Function F_0

The F_0 function is used for encryption and decryption. The function F_0 is defined as follows:

$F_0(x) = (x<<<_1) \oplus (x<<<_2) \oplus (x<<<_7)$

4.3 Function F_1

The F_1 function is used for encryption and decryption. The function F_1 is defined as follows:

$F_1(x) = (x<<<_3) \oplus (x<<<_4) \oplus (x<<<_6)$

5. HIGHT key schedule

The key scheduling part accepts a 128-bit master key $K = K_{15} \,//\, K_{14} \,//\, \cdots \,//\, K_0$ and yields 8 whitening key bytes WK_i and 128 subkey bytes SK_i, as shown below.

The generation of whitening keys is defined as follows.

for i = 0, 1, 2, 3:

$WK_i = K_{i+12}$

for i = 4, 5, 6, 7:

$WK_i = K_{i-4}$

The 128 subkeys are used for encryption and decryption, 4 subkeys per round. The generation of subkeys is defined as follows.

(1) $s_0 = 0$, $s_1 = 1$, $s_2 = 0$, $s_3 = 1$, $s_4 = 1$, $s_5 = 0$, $s_6 = 1$

$\delta_0 = s_6 \,||\, s_5 \,||\, s_4 \,||\, s_3 \,||\, s_2 \,||\, s_1 \,||\, s_0$

(2) for i = 1 to 127:

$s_{i+6} = s_{i+2} \oplus s_{i-1}$

$\delta_i = s_{i+6} \,||\, s_{i+5} \,||\, s_{i+4} \,||\, s_{i+3} \,||\, s_{i+2} \,||\, s_{i+1} \,||\, s_i$

(3) for i = 0 to 7:

for j = 0 to 7:

$SK_{16 \cdot i + j} = K_{j - i \bmod 8} \boxplus \delta_{16 \cdot i + j}$

for j = 0 to 7:

$SK_{16 \cdot i + j + 8} = K_{(j - i \bmod 8) + 8} \boxplus \delta_{16 \cdot i + j + 8}$