Network Working Group
INTERNET-DRAFT
Intended Status: Standard Track
Expires: December 26, 2011

B. Han
H. Lee
H. Jeong
Y. Won
KISA

June 24, 2011

# The HIGHT Encryption Algorithm
**draft-kisa-hight-00**

## Abstract

This document describes the HIGHT(HIGh security and light weigHT) encryption algorithm, which is suitable for low-resource device. HIGHT is a 64-bit block cipher with 128-bit keys. The algorithm consists of round functions, key schedule, encryption, and decryption.

## Status of this Memo

## Copyright and License Notice

## Table of Contents

## 1 Introduction

### 1.1. HIGHT overview

HIGHT is a 64-bit symmetric key light-weight block cipher suitable for low-resource device. HIGHT stands for 'HIGh security and light weigHT' and is developed by Korea 2005. HIGHT is a ISO/IEC international standard block cipher algorithm included in ISO/IEC 18033-3:2010 [ISO-HIGHT]. It has simple structure with use of basic arithmetic operation - XOR, addition/subtraction in modular 2**8, and circular shift rotation, and also without S-Box.

The features of HIGHT are outlined as follows:

- 64-bit input/output data block size
- 128-bit key length
- 32-round with XOR, modular addition, and shift rotation
- No S-Box
- Designed for low-resource device (data storage, power, etc.)

## 2. Notation and Terminology

The following notation is used in the description of HIGHT encryption algorithm:

| | |
|---|---|
| [^] | bitwise XOR |
| [+] | addition in modular 2**8 |
| [-] | subtraction in modular 2**8 |
| \|\| | concatenation |
| <<<n | left circular shift rotation by n-bit in 8-bit value |
| P | plaintext |
| C | ciphertext |
| K | master key |
| WK | whitening key |
| SK | subkey |
| F0 | round function 0 |
| F1 | round function 1 |
| Xi | i-th byte of X |
| Xj,i | i-th byte of X in round j |
| di | intermediate status value in subkey scheduling |

## 3. The HIGHT algorithm

### 3.1. Round functions

The HIGHT algorithm uses two round functions, namely, F0 and F1 which are now defined.

a) Round function 0 (F0)
The F0 function is used for encryption and decryption with 8-bit input. The function F0 is defined as follows:

```
     F0(x) = (x<<<1) [^] (x<<<2) [^] (x<<<7)
```

b) Round function 1 (F1)
The F1 function is used for encryption and decryption with 8-bit input. The function F1 is defined as follows:

```
     F1(x) = (x<<<3) [^] (x<<<4) [^] (x<<<6)
```

### 3.2. Key schedule

The key schedule for HIGHT describes the procedure to make whitening key bytes WKi and 128 subkey bytes SKi from a 128-bit master key K = K15 || K14 || ... || K0, as shown below.

a) The generation of whitening keys is defined as follows.

```
 for i = 0, 1, 2, 3:
     WKi = K(i+12)
 for i = 4, 5, 6, 7:
     WKi = K(i-4)
```

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

```
(1) s0 = 0, s1 = 1, s2 = 0, s3 = 1, s4 = 1, s5 = 0, s6 = 1
    d0 = s6 || s5 || s4 || s3 || s2 || s1 || s0

(2) for i = 1 to 127:
        s(i+6) = s(i+2) [^] s(i-1)
        di = s(i+6)||s(i+5)||s(i+4)||s(i+3)||s(i+2)||s(i+1)||si

(3) for i = 0 to 7:
    for j = 0 to 7:
        SK(16*i+j) = K(j-i mod 8) [+] d(16*i+j)
    for j = 0 to 7:
        SK(16*i+j+8) = K((j-i mod 8)+8) [+] d(16*i+j+8)
```

## 3.3. 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 = P7 || P6 || P5 || P4 || P3 || P2 || P1 || P0

  (2) X0,0 = P0 [+] WK0,          X0,1 = P1,
      X0,2 = P2 [^] WK1,          X0,3 = P3,
      X0,4 = P4 [+] WK2,          X0,5 = P5,
      X0,6 = P6 [^] WK3,          X0,7 = P7.

  (3) for i = 0 to 30:
        X(i+1),0 = Xi,7 [^] (F0(Xi,6)[+]SK(4*i+3)),  X(i+1),1 = Xi,0,
        X(i+1),2 = Xi,1 [+] (F1(Xi,0)[^]SK(4*i)),    X(i+1),3 = Xi,2,
        X(i+1),4 = Xi,3 [^] (F0(Xi,2)[+]SK(4*i+1)),  X(i+1),5 = Xi,4,
        X(i+1),6 = Xi,5 [+] (F1(Xi,4)[^]SK(4*i+2)),  X(i+1),7 = Xi,6.
      for i = 31:
        X(i+1),0 = Xi,0,      X(i+1),1 = Xi,1 [+] (F1(Xi,0)[^]SK124),
        X(i+1),2 = Xi,2,      X(i+1),3 = Xi,3 [^] (F0(Xi,2)[+]SK125),
        X(i+1),4 = Xi,4,      X(i+1),5 = Xi,5 [+] (F1(Xi,4)[^]SK126),
        X(i+1),6 = Xi,6,      X(i+1),7 = Xi,7 [^] (F0(Xi,6)[+]SK127).

  (4) C0 = X32,0 [+] WK4,         C1 = X32,1,
      C2 = X32,2 [^] WK5,         C3 = X32,3,
      C4 = X32,4 [+] WK6,         C5 = X32,5,
      C6 = X32,6 [^] WK7,         C7 = X32,7.

  (5) C = C7 || C6 || C5 || C4 || C3 || C2 || C1 || C0
```

## 3.4. 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 SKi and outputs of F0.

(2) The order in which the keys WKi and SKi are applied is reversed.

```
P7         P6      P5         P4      P3         P2      P1         P0
 |          |       |          |       |          |       |          |
 |         [^]-WK3  |         [^]-WK2  |         [^]-WK1  |     WK0-[^]
 |          |       |          |       |          |       |          |
X0,7       X0,6    X0,5       X0,4    X0,3       X0,2    X0,1      X0,0
 |          |       |          |       |          |       |          |
[^]-[+]-F0<-+      [+]-[^]-F1<-+      [^]-[+]-F0<-+      [+]-[^]-F1<-+
 |   |      |       |   |      |       |   |      |       |   |      |
 |  SK 3    |       |  SK2     |       |  SK1     |       |  SK0     |
 \          /       /          /       /          /       /          /
  ---------/-------/----------/-------/----------/-------/---------\/
  ________/  _____/  ________/  _____/  ________/  _____/  ________/\
 /          /       /          /       /          /       /          \
X1,7       X1,6    X1,5       X1,4    X1,3       X1,2    X1,1      X1,0
 |          |       |          |       |          |       |          |
[^]-[+]-F0<-+      [+]-[^]-F1<-+      [^]-[+]-F0<-+      [+]-[^]-F1<-+
 |   |      |       |   |      |       |   |      |       |   |      |
 |  SK7     |       |  SK6     |       |  SK5     |       |  SK4     |
 \          /       /          /       /          /       /          /
  ---------/-------/----------/-------/----------/-------/---------\/
  ________/  _____/  ________/  _____/  ________/  _____/  ________/\
 /          /       /          /       /          /       /          \
X2,7       X2,6    X2,5       X2,4    X2,3       X2,2    X2,1      X2,0
 :          :       :          :       :          :       :          :
 :          :       :          :       :          :       :          :
 :          :       :          :       :          :       :          :
X31,7     X31,6   X31,5      X31,4   X31,3      X31,2   X31,1     X31,0
 |          |       |          |       |          |       |          |
[^]-[+]-F0<-+      [+]-[^]-F1<-+      [^]-[+]-F0<-+      [+]-[^]-F1<-+
 |   |      |       |   |      |       |   |      |       |   |      |
 | SK127    |       | SK126    |       | SK125    |       | SK12     |
 |          |       |          |       |          |       |          |
X32,7     X32,6   X32,5      X32,4   X32,3      X32,2   X32,1     X32,0
 |          |       |          |       |          |       |          |
 |         [^]-WK7  |         [^]-WK6  |         [^]-WK5  |     WK4-[^]
 |          |       |          |       |          |       |          |
C7         C6      C5         C4      C3         C2      C1         C0
```

Figure 1. Encryption procedure of HIGHT

### 3.5. HIGHT Object Identifiers

For those who may be using HIGHT in algorithm negotiation within a protocol, or in any other context that may require the use of Object Identifiers (OIDs), the following OIDs have been defined.

```
  algorithm OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
            kisa(200004) algorithm(1) }

  id-hight OBJECT IDENTIFIER ::= { algorithm hight(40) }

  id-hightECB OBJECT IDENTIFIER ::= { algorithm hightECB(41) }

  id-hightCBC OBJECT IDENTIFIER ::= { algorithm hightCBC(42) }

  id-hightCFB OBJECT IDENTIFIER ::= { algorithm hightCFB(43) }

  id-hightOFB OBJECT IDENTIFIER ::= { algorithm hightOFB(44) }

  id-hightCTR OBJECT IDENTIFIER ::= { algorithm hightCTR(45) }
```

The id-hightECB, id-hightCBC, id-hightCFB, id-hightOFB, and id-hightCTR OIDs are used when Electronic CodeBook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feed-Back (CFB) mode, Output Feed-Back (OFB) mode, and Counter (CTR) mode of operation based on the HIGHT block cipher is provided respectively.

## 4. Security Considerations

No security problem has been found on HIGHT.

## 5. Test Vectors

### 5.1. Test vectors 1

```
Key :           00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Plaintext :     00 00 00 00 00 00 00 00
Ciphertext :    00 f4 18 ae d9 4f 03 f2
```

<table>
<tr><th>Sub Key</th><th>Value</th><th>Sub Key</th><th>Value</th></tr>
<tr><td>SK3 ||SK2 ||SK1 ||SK0</td><td>= e7135b59,</td><td>SK67 ||SK66 ||SK65 ||SK64</td><td>= cfa7c7f6</td></tr>
<tr><td>SK7 ||SK6 ||SK5 ||SK4</td><td>= c99cb0c8,</td><td>SK71 ||SK70 ||SK69 ||SK68</td><td>= 48555f62</td></tr>
<tr><td>SK11||SK10||SK9 ||SK8</td><td>= 906d96d7,</td><td>SK75 ||SK74 ||SK73 ||SK72</td><td>= 1f50a1b1</td></tr>
<tr><td>SK15||SK14||SK13||SK12</td><td>= 2c6a5599,</td><td>SK79 ||SK78 ||SK77 ||SK76</td><td>= a5986d86</td></tr>
<tr><td>SK19||SK18||SK17||SK16</td><td>= 27032ade,</td><td>SK83 ||SK82 ||SK81 ||SK80</td><td>= 0706f33c</td></tr>
<tr><td>SK23||SK22||SK21||SK20</td><td>= b5e32d31,</td><td>SK87 ||SK86 ||SK85 ||SK84</td><td>= fb2b7aff</td></tr>
<tr><td>SK27||SK26||SK25||SK24</td><td>= ced9de4e,</td><td>SK91 ||SK90 ||SK89 ||SK88</td><td>= 7a755a93</td></tr>
<tr><td>SK31||SK30||SK29||SK28</td><td>= 48919180,</td><td>SK95 ||SK94 ||SK93 ||SK92</td><td>= 7bb39134</td></tr>
<tr><td>SK35||SK34||SK33||SK32</td><td>= f915b5f4,</td><td>SK99 ||SK98 ||SK97 ||SK96</td><td>= bcdf15f0</td></tr>
<tr><td>SK39||SK38||SK37||SK36</td><td>= fadc0ee2,</td><td>SK103||SK102||SK101||SK100</td><td>= ef018ca2</td></tr>
<tr><td>SK43||SK42||SK41||SK40</td><td>= bba15439,</td><td>SK107||SK106||SK105||SK104</td><td>= 2a436495</td></tr>
<tr><td>SK47||SK46||SK45||SK44</td><td>= 9fadb9bf,</td><td>SK111||SK110||SK109||SK108</td><td>= ae882255</td></tr>
<tr><td>SK51||SK50||SK49||SK48</td><td>= 16b7f8e8,</td><td>SK115||SK114||SK113||SK112</td><td>= c7e50f52</td></tr>
<tr><td>SK55||SK54||SK53||SK52</td><td>= e41e0239,</td><td>SK119||SK118||SK117||SK116</td><td>= 67d9bcf0</td></tr>
<tr><td>SK59||SK58||SK57||SK56</td><td>= d9451b36,</td><td>SK123||SK122||SK121||SK120</td><td>= 61a18fda</td></tr>
<tr><td>SK63||SK62||SK61||SK60</td><td>= a9b0ad97,</td><td>SK127||SK126||SK125||SK124</td><td>= d1357c79</td></tr>
</table>

| Round | Value | Round | Value |
|---|---|---|---|
| Initial | 0000001100220033 | Round 17 | 2c93a90ddd0283ae |
| Round 1 | 00ce1138223f33e7 | Round 18 | 93570db102d9aec4 |
| Round 2 | cee138ef3fa3e78a | Round 19 | 57b7b1dbd998c4e4 |
| Round 3 | e14fef91a3708a8a | Round 20 | b7bedb55989ae458 |
| Round 4 | 4f8a91cd70518ad1 | Round 21 | be87559d9a515868 |
| Round 5 | 8a53cd0951c3d1ee | Round 22 | 87ce9d5351786873 |
| Round 6 | 534609c7c3e4ee7d | Round 23 | ceab53d6784b73bc |
| Round 7 | 4673c7c5e41b7dd7 | Round 24 | ab30d6d74ba8bc69 |
| Round 8 | 7359c58c1b33d79c | Round 25 | 30bfd7f7a83369df |
| Round 9 | 595f8cf333d59c07 | Round 26 | bf13f71733bfdf7d |
| Round 10 | 5f0cf317d507073f | Round 27 | 134617f1bfd57db2 |
| Round 11 | 0ca0173007033fb6 | Round 28 | 467bf187d5c4b277 |
| Round 12 | a03a3043030bb63e | Round 29 | 7b3187d2c4f5772b |
| Round 13 | 3a7943b40b2b3e37 | Round 30 | 315dd246f5482bde |
| Round 14 | 7920b47a2b7c37b5 | Round 31 | 5d3846d148a1def3 |
| Round 15 | 20637a797ce4b5d0 | Round 32 | 003818d1d9a103f3 |
| Round 16 | 632c79a9e4ddd083 | Final | 00f418aed94f03f2 |

### 5.2. Test vectors 2

Key :           ff ee dd cc bb aa 99 88 77 66 55 44 33 22 11 00
Plaintext :     00 11 22 33 44 55 66 77
Ciphertext :    23 ce 9f 72 e5 43 e6 d8

| Sub Key | Value | Sub Key | Value |
|---|---|---|---|
| SK3 \|\|SK2 \|\|SK1 \|\|SK0 | = 4e587e5a, | SK67 \|\|SK66 \|\|SK65 \|\|SK64 | = be74727f |
| SK7 \|\|SK6 \|\|SK5 \|\|SK4 | = b8695b51, | SK71 \|\|SK70 \|\|SK69 \|\|SK68 | = af9a8263 |
| SK11\|\|SK10\|\|SK9 \|\|SK8 | = 07c2c9e8, | SK75 \|\|SK74 \|\|SK73 \|\|SK72 | = 1e2d5c4a |
| SK15\|\|SK14\|\|SK13\|\|SK12 | = 2b471032, | SK79 \|\|SK78 \|\|SK77 \|\|SK76 | = 1ceda097 |
| SK19\|\|SK18\|\|SK17\|\|SK16 | = 6c262bcd, | SK83 \|\|SK82 \|\|SK81 \|\|SK80 | = d4b17ca3 |
| SK23\|\|SK22\|\|SK21\|\|SK20 | = 828eb698, | SK87 \|\|SK86 \|\|SK85 \|\|SK84 | = 404e7bee |
| SK27\|\|SK26\|\|SK25\|\|SK24 | = 230cef4d, | SK91 \|\|SK90 \|\|SK89 \|\|SK88 | = 5730f30a |
| SK31\|\|SK30\|\|SK29\|\|SK28 | = 254c2af7, | SK95 \|\|SK94 \|\|SK93 \|\|SK92 | = d0e6a233 |
| SK35\|\|SK34\|\|SK33\|\|SK32 | = 1c16a4c1, | SK99 \|\|SK98 \|\|SK97 \|\|SK96 | = 67687c35 |
| SK39\|\|SK38\|\|SK37\|\|SK36 | = a5657527, | SK103\|\|SK102\|\|SK101\|\|SK100 | = 12027b6f |
| SK43\|\|SK42\|\|SK41\|\|SK40 | = eeb25316, | SK107\|\|SK106\|\|SK105\|\|SK104 | = e5dcdbea |
| SK47\|\|SK46\|\|SK45\|\|SK44 | = 5a463014, | SK111\|\|SK110\|\|SK109\|\|SK108 | = e1992132 |
| SK51\|\|SK50\|\|SK49\|\|SK48 | = 17a6c593, | SK115\|\|SK114\|\|SK113\|\|SK112 | = 504c5475 |
| SK55\|\|SK54\|\|SK53\|\|SK52 | = 6d85475c, | SK119\|\|SK118\|\|SK117\|\|SK116 | = 68c8899b |
| SK59\|\|SK58\|\|SK57\|\|SK56 | = ea44f8f1, | SK123\|\|SK122\|\|SK121\|\|SK120 | = fa18e40d |
| SK63\|\|SK62\|\|SK61\|\|SK60 | = 422702ca, | SK127\|\|SK126\|\|SK125\|\|SK124 | = e2345934 |

| Round | Value | Round | Value |
|---|---|---|---|
| Initial | 00ee222144886643 | Round 17 | db63ca6b6e9dfaaf |
| Round 1 | ee2d21b1880a435f | Round 18 | 63776b6b9d09af72 |
| Round 2 | 2db4b11c0acc5fde | Round 19 | 77856b93091172c5 |
| Round 3 | b4951c9fcca3dec5 | Round 20 | 851793871106c58c |
| Round 4 | 95c19fe4a30fc556 | Round 21 | 17a7878206f18c48 |
| Round 5 | c115e4730f545645 | Round 22 | a7598251f1c64855 |
| Round 6 | 15e27386540d45b7 | Round 23 | 597d5119c6e85575 |
| Round 7 | e26486c30dabb777 | Round 24 | 7d4a196ee8e775d8 |
| Round 8 | 6424c35bab9d7772 | Round 25 | 4a7f6ef7e7bdd882 |
| Round 9 | 24725b8c9d607282 | Round 26 | 7fadf729bdcb8284 |
| Round 10 | 72458c7b602d829d | Round 27 | ad442985cb29845f |
| Round 11 | 458c7bab2dc69d59 | Round 28 | 44b58548296e5f31 |
| Round 12 | 8cc6ab08c6ba5982 | Round 29 | b51d488f6e0231f3 |
| Round 13 | c60f0841ba688280 | Round 30 | 1df78ff802f8f39d |
| Round 14 | 0fd3413668f280d4 | Round 31 | f7fdf850f8529dd8 |
| Round 15 | d35c3627f2afd4e4 | Round 32 | 23fd9f50e552e6d8 |
| Round 16 | 5cdb27caaf6ee4fa | Final | 23ce9f72e543e6d8 |

## 6. References

### 6.1. Normative References

[ISO-HIGHT] ISO/IEC, "Information technology - Security techniques - Encryption - Part 3: Block ciphers", ISO/IEC 18033-3, December 2010.

Authors' Addresses

Byoungjin Han
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: labon58@gmail.com, bjhan@kisa.or.kr

Hwanjin Lee
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: lhj79@kisa.or.kr

Hyuncheol Jeong
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: hcjung@kisa.or.kr

Yoojae Won
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: yjwon@kisa.or.kr