Specification of Hulk cipher

May 13, 2019

Written by Gilad Eini – giladeini@gmail.com

1. **Hulk Cipher**
   - Block size: 64-bit
   - Key size: 64 bit
   - Hulk is based on a feistel network with 4-bit sboxes, a bit permutation as the linear layer and rotation. See Figure below for a visual representation.
   - Hulk was assembled from several sources
     - Sbox from 'Present' cipher
     - Sigma from TC05
     - Key schedule based on TC05
       - Expanded to 32 bits rks
     - F was not copied
     - Round function from TC05
     - Encrypt\Decrypt from TC05
2. Round Function(L, R, rki) s.t. |L| = |R| = |rki| = 32bits
   - *let* S be the sbox s.t.
     - S = (0xC, 0x5, 0x6, 0xB, 0x9, 0x0, 0xA, 0xD, 0x3, 0xE, 0xF, 0x8, 0x4, 0x7, 0x1, 0x2)
   - *let* σ be a bit *permutation* s.t.

$$\sigma = \left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 6 & 0 & 1 & 7 & E & 8 & 9 & F & 2 & 4 & 5 & 3 & A & C & D & B \end{array}\right)$$

   - *let* $F(W = l|r)$ s.t. |l| = |r| = 16bits
     - $X = l'|r' = rotateRight8Bits(\sigma(S(l)) \mid \sigma(S(r)))$
     - $W' = (\ \sigma(l') \mid \sigma(r')$
   - So the round function does
     - $L' = F(L) \oplus R \ \oplus rki$
     - R' = L
     - Return L', R'
3. **Key schedule**
   - Given a 64 bit key K, slice it to 16bits subkeys s.t. K=k0,k1,k2,k3
   - RKs <- Create 'rounds' + 1 16bits subkeys s.t.
     - $rk_{i+1} = rk_{i-3} \oplus rk_i \oplus \sigma(rk_{i-1}) \oplus 0xC$
   - RK's <- Create 'rounds' 32bits subkeys s.t.
     - $rk'_i = rk_i \mid rk_{i+1}$
   - Keep the RK's (discard RKs)

4. Test Vectors

Plaintext	Cipher	Key
0x0000000000000000	0x0000000000000000	0x87B8FD1C16C7837E
0x0000000012345678	0x1234567890ABCDEF	0x8BA17C400F14946E
0x123456789ABCDEF0	0x123456789ABCDEF0	0x3693CFE187272D28

5. Hulk cipher visual representation