Linear cryptanalysis of NUSH block cipher

WU Wenling (吴文玲) & FENG Dengguo (冯登国)

State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China; Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing 100080, China

Correspondence should be addressed to Wu Wenling (email: wwl@ercist.iscas.ac.cn)

Received July 23, 2001

Abstract NUSH is a block cipher as a candidate for NESSIE. NUSH is analyzed by linear cryptanalysis. The complexity $\delta = (\varepsilon, \eta)$ of the attack consists of data complexity ε and time complexity η. Three linear approximations are used to analyze NUSH with 64-bit block. When $|K| = 128$ bits, the complexities of three attacks are $(2^{58}, 2^{124})$, $(2^{60}, 2^{78})$ and $(2^{62}, 2^{55})$ respectively. When $|K| = 192$ bits, the complexities of three attacks are $(2^{58}, 2^{157})$ $(2^{60}, 2^{96})$ and $(2^{62}, 2^{58})$ respectively. When $|K| = 256$ bits, the complexities of three attacks are $(2^{58}, 2^{125})$, $(2^{60}, 2^{78})$ and $(2^{62}, 2^{53})$ respectively. Three linear approximations are used to analyze NUSH with 128-bit block. When $|K| = 128$ bits, the complexities of three attacks are $(2^{122}, 2^{95})$, $(2^{124}, 2^{57})$ and $(2^{126}, 2^{52})$ respectively. When $|K| = 192$ bits, the complexities of three attacks are $(2^{122}, 2^{142})$, $(2^{124}, 2^{75})$ and $(2^{126}, 2^{58})$ respectively. When $|K| = 256$ bits, the complexities of three attacks are $(2^{122}, 2^{168})$, $(2^{124}, 2^{81})$ and $(2^{126}, 2^{64})$ respectively. Two linear approximations are used to analyze NUSH with 256-bit block. When $|K| = 128$ bits, the complexities of two attacks are $(2^{252}, 2^{122})$ and $(2^{254}, 2^{119})$ respectively. When $|K| = 192$ bits, the complexities of two attacks are $(2^{252}, 2^{181})$ and $(2^{254}, 2^{177})$ respectively. When $|K| = 256$ bits, the complexities of two attacks are $(2^{252}, 2^{240})$ and $(2^{254}, 2^{219})$ respectively. These results show that NUSH is not immune to linear cryptanalysis, and longer key cannot enhance the security of NUSH.

Keywords: **block cipher, linear cryptanalysis, linear approximation.**

NUSH[1] is a block cipher designed by Lebedev and Volchkov as a candidate for NESSSIE. It has no S-boxes, and it achieves "confusion" and "diffusion" by using different operations. Its block length N is variable. N can be 64, 128 or 256 bits, and its key length can be 128, 192 or 256 bits. It has 36, 68 or 132 rounds, depending on the block length N. NUSH is studied in this paper. The results show that NUSH is not immune to linear cryptanalysis[2], and longer key cannot enhance the security of NUSH. For convenience, we present the encryption algorithm and key schedule of NUSH.

Encryption algorithm

First an N-bit plaintext P is separated into four $n = N/4$-bit data $P_3P_2P_1P_0$, which is XORed with subkeys $KS_0KS_1KS_2KS_3$, and marked $a_0b_0c_0d_0$. Then, the following operations are performed from $i = 1$ to $r - 1$.

$$\begin{aligned} a_i &= b_{i-1}, \\ b_i &= (((c_{i-1} \oplus (KR_{i-1} + C_{i-1})) + b_{i-1})\rangle\rangle\rangle S_{i-1}, \\ c_i &= d_{i-1}, \\ d_i &= a_{i-1} + (b_i \# d_{i-1}). \end{aligned} \tag{0.1}$$

For the last round $i = r$, the following is carried out.

$$\begin{aligned} a_r &= a_{r-1} + (c_r \# d_{r-1}), \\ b_r &= b_{r-1}, \\ c_r &= (((c_{r-1} \oplus (KR_{r-1} + C_{r-1})) + b_{r-1})\rangle\rangle\rangle S_{r-1}, \\ d_r &= d_{r-1}. \end{aligned} \tag{0.2}$$

Finally, $a_r b_r c_r d_r$ is XORed with subkeys $KF_0 KF_1 KF_2 KF_3$. The resultant value is the ciphertext $M = M_0 M_1 M_2 M_3$, where C_i and S_i are fixed constants, " # " is "AND" or "OR", which are chosen by fixed tables.

Key schedule

The master key is represented by n-bit words of the form $(K[0], K[1], \cdots)$ and the least bit of the word $K[0]$ is the least bit of key.

When $N = 64$ $(n = 16)$ and $|K| = 128$, $KS_0 = K[4]$, $KS_1 = K[5]$, $KS_2 = K[6]$, $KS_3 = K[7]$, $KF_0 = K[3]$, $KF_1 = K[2]$, $KF_2 = K[1]$, $KF_3 = K[0]$, $KR_i = K[\text{imod8}]\, i = 0, \cdots, 35$.

When $N = 64$ $(n = 16)$ and $|K| = 192$, $KS_0 = K[4]$, $KS_1 = K[5]$, $KS_2 = K[6]$, $KS_3 = K[7]$, $KF_0 = K[11]$, $KF_1 = K[10]$, $KF_2 = K[9]$, $KF_3 = K[8]$, $KR_i = K[\text{imod12}]\, i = 0, \cdots, 35$.

When $N = 64$ $(n = 16)$ and $|K| = 256$, $KS_0 = K[12]$, $KS_1 = K[13]$, $KS_2 = K[14]$, $KS_3 = K[15]$, $KF_0 = K[13]$, $KF_1 = K[12]$, $KF_2 = K[15]$, $KF_3 = K[14]$, $KR_i = K[\text{imod16}]\, i = 0, \cdots, 35$.

When $N = 128$ $(n = 32)$ and $|K| = 128$, $KS_0 = K[3]$, $KS_1 = K[2]$, $KS_2 = K[1]$, $KS_3 = K[0]$, $KF_0 = K[1]$, $KF_1 = K[0]$, $KF_2 = K[3]$, $KF_3 = K[2]$, $KR_i = K[\text{imod4}]\, i = 0, \cdots, 67$.

When $N = 128$ $(n = 32)$ and $|K| = 192$, $KS_0 = K[2]$, $KS_1 = K[3]$, $KS_2 = K[4]$, $KS_3 = K[5]$, $KF_0 = K[5]$, $KF_1 = K[4]$, $KF_2 = K[3]$, $KF_3 = K[2]$, $KR_i = K[\text{imod6}]\, i = 0, \cdots, 67$.

When $N = 128$ $(n = 32)$ and $|K| = 256$, $KS_0 = K[4]$, $KS_1 = K[5]$, $KS_2 = K[6]$, $KS_3 = K[7]$, $KF_0 = K[5]$, $KF_1 = K[4]$, $KF_2 = K[7]$, $KF_3 = K[6]$, $KR_i = K[\text{imod8}]\, i = 0, \cdots, 67$.

When $N = 256$ $(n = 64)$ and $|K| = 128$, $KS_0 = K[1]$, $KS_1 = K[0]$, $KS_2 = K[1]$, $KS_3 = K[0]$, $KF_0 = K[0]$, $KF_1 = K[1]$, $KF_2 = K[0]$, $KF_3 = K[1]$, $KR_i = K[\text{imod2}]\, i = 0, \cdots, 131$.

When $N = 256$ $(n = 64)$ and $|K| = 192$, $KS_0 = K[2]$, $KS_1 = K[1]$, $KS_2 = K[0]$, $KS_3 = K[2]$, $KF_0 = K[1]$, $KF_1 = K[2]$, $KF_2 = K[2]$, $KF_3 = K[0]$, $KR_i = K[\text{imod3}]\, i = 0, \cdots, 131$.

When $N = 256$ $(n = 64)$ and $|K| = 256$, $KS_0 = K[3]$, $KS_1 = K[2]$, $KS_2 = K[1]$, $KS_3 = K[0]$, $KF_0 = K[2]$, $KF_1 = K[3]$, $KF_2 = K[0]$, $KF_3 = K[1]$, $KR_i = K[\text{imod4}]\, i = 0, \cdots, 131$.

1 NUSH with 64-bit block

1.1 Linear approximation of round function

From eq. (0.1), we can get

$$a_i = b_{i-1}, \tag{1.1}$$

$$d_i = a_{i-1} + (b_i \# d_{i-1}). \tag{1.2}$$

From eq. (1.1), we have the following linear approximation with probability 1:

$$a_i[0] = b_{i-1}[0]. \tag{1.3}$$

Let $f(x, y) = x \# y$ be a Boolean function. It is easy to validate that $f(x, y) = l(x, y) = x \oplus y$ holds with probability $p = 0.75$ or 0.25. So for eq. (1.2) we have the following linear approximation with probability 0.75 or 0.25:

$$d_i[0] = a_{i-1}[0] \oplus b_i[0] \oplus d_{i-1}[0]. \tag{1.4}$$

By using eqs. (1.3) and (1.4), we can get the following linear approximation of round function whose probability p is 0.75;

$$a_i[0] \oplus b_i[0] \oplus d_i[0] = a_{i-1}[0] \oplus b_{i-1}[0] \oplus d_{i-1}[0] \oplus \theta. \tag{1.5}$$

$\theta = 0$ if # is "AND", $\theta = 1$ if # is "OR". It is noticed that eq. (1.5) is independent of the key.

1.2 Relationship among middle value and plaintext and ciphertext and key

1.2.1 Relationship among $a_1[0] \oplus b_1[0] \oplus d_1[0]$ and plaintext and key. Let $a_1 b_1 c_1 d_1$ be the output of the first round. From eq. (0.1), we have

$$\begin{aligned} a_1 &= b_0, \\ b_1 &= (((c_0 \oplus (KR_0 + C_0)) + b_0)) \gg\gg S_0, \\ c_1 &= d_0, \\ d_1 &= a_0 + (b_i \# d_0). \end{aligned}$$

As $S_0 = 4$, $b_1[0]$ depends on $c_0[0—4]$, $b_0[0—4]$, $KR_0[0—4]$ and $C_0[0—4]$. Here $b_0[0—4]$ denotes the least five bits of b_0. Hence $a_1[0] \oplus b_1[0] \oplus d_1[0]$ depends on $a_0[0]$, $b_0[0—4]$, $c_0[0—4]$, $d_0[0]$, $KR_0[0—4]$ and $C_0[0—4]$. Because $a_0 b_0 c_0 d_0 = P_3 P_2 P_1 P_0 \oplus KS_0 KS_1 KS_2 KS_3$, $C_0[0—4]$ is constant, $a_1[0] \oplus b_1[0] \oplus d_1[0]$ depends only on $P_3[0] \oplus KS_0[0]$, $P_2[0—4] \oplus KS_1[0—4]$, $P_1[0—4] \oplus KS_2[0—4]$, $P_0[0] \oplus KS_3[0]$ and $KR_0[0—4]$. Here the relationship among them is expressed by function f_1:

$$\begin{aligned} a_1[0] \oplus b_1[0] \oplus d_1[0] = f_1(&P_0[0], P_1[0—4], P_2[0—4], P_3[0], \\ &KS_0[0], KS_1[0—4], KS_2[0—4], KS_3[0], KR_0[0—4]). \end{aligned} \tag{1.6}$$

1.2.2 Relationship among $a_2[0] \oplus b_2[0] \oplus d_2[0]$ and plaintext and key. Similarly, it can be proved that $a_2[0] \oplus b_2[0] \oplus d_2[0]$ depends only on $P_3[0] \oplus KS_0[0]$, $P_2[0—11] \oplus KS_1[0—11]$, $P_1[0—11] \oplus KS_2[0—11]$, $P_0[0—7] \oplus KS_3[0—7]$, $KR_0[0—11]$ and $KR_1[0—7]$. The relationship among them is expressed by function f_2:

$$\begin{aligned} a_2[0] \oplus b_2[0] \oplus d_2[0] = f_2(&P_0[0—7], P_1[0—11], P_2[0—11], P_3[0], KS_0[0], \\ &KS_1[0—11], KS_2[0—11], KS_3[0—7], KR_0[0—11], KR_1[0—7]). \end{aligned} \tag{1.7}$$

1.2.3 Relationship among $a_3[0]\oplus b_3[0]\oplus d_3[0]$ and plaintext and key. Similarly, it can be proved that $a_3[0]\oplus b_3[0]\oplus d_3[0]$ depends only on plaintext P, $KS_0[0—11]$, KS_1, KS_2, KS_3, KR_0, KR_1 and $KR_2[0—11]$. Here the relationship among them is expressed by function f_3:

$$a_3[0]\oplus b_3[0]\oplus d_3[0] = f_3(P,\ KS_0[0—11],\ KS_1,\ KS_2,\ KS_3,\ KR_0,\ KR_1,\ KR_2[0—11]). \tag{1.8}$$

1.2.4 Relationship among $a_{32}[0]\oplus b_{32}[0]\oplus d_{32}[0]$ and ciphertext and key. From eq. (0.1), we have

$$a_{32}[0] = d_{33}[0]\oplus(b_{33}[0]\&c_{33}[0]),$$
$$b_{32}[0] = a_{33}[0],$$
$$d_{32}[0] = c_{33}[0].$$

Hence $a_{32}[0]\oplus b_{32}[0]\oplus d_{32}[0]$ depends only on $a_{33}[0]b_{33}[0]c_{33}[0]d_{33}[0]$.

From eq. (0.1), we have

$$a_{33}[0] = d_{34}[0]\oplus(b_{34}[0]\ \#\ c_{34}[0]),$$
$$b_{33}[0] = a_{34}[0],$$
$$d_{33}[0] = c_{34}[0],$$
$$b_{34} = (b_{33} + (c_{33}\oplus(KR_{33} + C_{33})))\gg\gg\gg 15.$$

So $(b_{34}\lll\lll(15))[0] = b_{33}[0]\oplus c_{33}[0]\oplus(KR_{33} + C_{33})[0]$, $c_{33}[0] = b_{34}[1]\oplus b_{33}[0]\oplus KR_{33}[0]\oplus C_{33}[0]$. Therefore $a_{33}[0]b_{33}[0]c_{33}[0]d_{33}[0]$ depends on $a_{34}[0]b_{34}[0,1]c_{34}[0]d_{34}[0]$ and $KR_{33}[0]$.

From eq. (0.1), we have

$$a_{34}[0] = d_{35}[0]\oplus(b_{35}[0]\ \#\ c_{35}[0]),$$
$$b_{34}[0,1] = a_{35}[0,1],$$
$$d_{34}[0] = c_{35}[0],$$
$$b_{35} = (b_{34} + (c_{34}\oplus(KR_{34}[0]\oplus C_{34})))\gg\gg\gg 4.$$

So $(b_{35}\lll\lll(4))[0] = b_{34}[0]\oplus c_{34}[0]\oplus KR_{34}[0]\oplus C_{34}[0]$, $c_{34}[0] = b_{34}[0]\oplus b_{35}[12]\oplus KR_{34}[0]\oplus C_{34}[0]$. Therefore $a_{34}[0]b_{34}[0,1]c_{34}[0]d_{34}[0]$ depends on $a_{35}[0,1]b_{35}[0,12]c_{35}[0]d_{35}[0]$ and $KR_{34}[0]$.

From eq. (0.1), we get

$$a_{36}[0,1] = a_{35}[0,1] + (c_{36}[0,1]\ \#\ d_{36}[0,1]),$$
$$b_{36}[0,12] = b_{35}[0,12],$$
$$d_{36}[0] = d_{35}[0],$$
$$c_{36} = (b_{36} + (c_{35}\oplus(KR_{35} + C_{35})))\gg\gg\gg 14.$$

So $(c_{36}\lll\lll(14))[0] = b_{36}[0]\oplus c_{35}[0]\oplus KR_{35}[0]\oplus C_{35}[0]$, $c_{35}[0] = b_{36}[0]\oplus c_{36}[2]\oplus KR_{35}[0]\oplus C_{35}[0]$. Therefore, $a_{35}[0,1]b_{35}[0,12]c_{35}[0]d_{35}[0]$ depends on $a_{36}[0,1]b_{36}[0,$

$12]c_{36}[0,1,2]d_{35}[0,1]$ and $KR_{35}[0]$.

From the above discussion, it is shown that $a_{32}[0]\oplus b_{32}[0]\oplus d_{32}(0)'$ depends on $M_3[0,1]$, $M_2[0,12]$, $M_1[0—2]$, $M_0[0,1]$, $KF_0[0,1]$, $KF_1[0,12]$, $KF_2[0—2]$, $KF_3[0,1]$, $KR_{33}[0]$, $KR_{34}[0]$ and $KR_{35}[0]$. Here the relationship among them is expressed by function f_4:

$$a_{32}[0]\oplus b_{32}[0]\oplus d_{32}[0] = f_4(M_0[0,1], M_1[0—2], M_2[0,12], M_3[0,1], KF_0[0,1], KF_1[0,12], KF_2[0—2], KF_3[0,1], KR_{33}[0], KR_{34}[0], KR_{35}[0]). \quad (1.9)$$

1.2.5 Relationship among $a_{31}[0]\oplus b_{31}[0]\oplus d_{31}[0]$ and ciphertext and key. As discussed in subsec. 1.2.4, it is shown that $a_{31}[0]\oplus b_{31}[0]d_{31}[0]$ depends on $M_3[0,1]M_2[0—9, 12]M_1[0—11]M_0[0—9]$, $KF_0[0,1]$, $KF_1[0—9, 12]$, $KF_2[0—11]$, $KF_3[0—9]$, $KR_{32}[0]$, $KR_{33}[0]$, $KR_{34}[0]$ and $KR_{35}[0—9]$. Here the relationship among them is expressed by function f_5:

$$\begin{aligned} a_{31}[0]\oplus b_{31}[0]\oplus d_{31}[0] = f_5(&M_0[0—9], M_1[0—11], M_2[0—9, 12],\\ &M_3[0,1], KF_0[0,1], KF_1[0—9,12], KF_2[0—11],\\ &KF_3[0—9], KR_{32}[0], KR_{33}[0], KR_{34}[0], KR_{35}[0—9]). \end{aligned} \quad (1.10)$$

1.3 Linear cryptanalysis to NUSH with 64-bit block

1.3.1 Linear cryptanalysis by 29-round linear approximation. By applying eq. (1.5), we see the following 29-round linear approximation which holds with probability $1/2+2^{-30}$:

$$a_2[0]\oplus b_2[0]\oplus d_2[0] = a_{31}[0]\oplus b_{31}[0]\oplus d_{31}[0]. \quad (1.11)$$

By using eqs. (1.7) and (1.10), we can express eq. (1.11) with plaintext, ciphertext and key.

$$\begin{aligned} &f_2(P, KS_0[0], KS_1[0—11], KS_2[0—11], KS_3[0—7], KR_0[0—11], KR_1[0—7])\\ &= f_5(M, KF_0[0,1], KF_1[0—9,12], KF_2[0—11], KF_3[0—9], KR_{32}[0],\\ &\quad KR_{33}[0], KR_{34}[0], KR_{35}[0—9]). \end{aligned} \quad (1.12)$$

From key schedule of NUSH, it is known that eq. (1.12) contains m_0-bit key, m_0 is 78 when $|K|$ = 128-bit, m_0 is 96 when $|K|$ = 192-bit, m_0 is 78 when $|K|$ = 256-bit. So we can determine m_0-bit key by the following algorithm based on the results in ref. [2].

Algorithm

Step 1. For each candidate m_0-bit key K^i ($i = 1, \cdots, 2^{m_0}$), let T_i be the number of plaintexts such that eq. (1.12) holds.

Step 2. If T_t is the maximal value of all T_i's, then adopt the key candidate K^t.

Step 3. Deduce the remaining key bits by using similar reduced round linear approximations or by exhausting.

The data complexity of this attack is about 2^{60}. For 128-bit, 192-bit and 256-bit key, the time complexity is about 2^{78}, 2^{96} and 2^{78} respectively.

1.3.2 Linear cryptanalysis by 30-round linear approximations. By applying eq. (1.5), we

obtain the following two 30-round linear approximations which holds with probability $1/2 + 2^{-31}$:

$$a_2[0] \oplus b_2[0] \oplus d_2[0] = a_{32}[0] \oplus b_{32}[0] \oplus d_{32}[0] \oplus 1, \quad (1.13)$$

$$a_1[0] \oplus b_1[0] \oplus d_1[0] = a_{31}[0] \oplus b_{31}[0] \oplus d_{31}[0]. \quad (1.14)$$

By using eqs. (1.7) and (1.9), we can express eq. (1.13) with plaintext, ciphertext and key.

$$f_2(P, KS_0[0], KS_1[0—11], KS_2[0—11], KS_3[0—7], KR_0[0—11], KR_1[0—7]) \oplus 1$$
$$= f_4(M, KF_0[0,1], KF_1[0,12], KF_2[0—2], KF_3[0,1], KR_{33}[0], KR_{34}[0], KR_{35}[0]). \quad (1.15)$$

By using eqs. (1.6) and (1.10), we can express eq. (1.14) with plaintext, ciphertext and key.

$$f_1(P, KS_0[0], KS_1[0—4], KS_2[0—4], KS_3[0], KR_0[0—4])$$
$$= f_5(M, KF_0[0,1], KF_1[0—9,12], KF_2[0—11], KF_3[0—9],$$
$$KR_{32}[0], KR_{33}[0], KR_{34}[0], KR_{35}[0—9]). \quad (1.16)$$

From key schedule of NUSH, for 128-bit, 192-bit and 256-bit key, it is known that eq. (1.15) contains 57, 62 and 56 bits key respectively, eq. (1.16) contains 55, 58 and 53 bits key respectively.

By using linear approximation (1.15), the data complexity of linear cryptanalysis is about 2^{62}, the time complexity is about 2^{57}, 2^{62} and 2^{56} respectively for 128-bit, 192-bit and 256-bit key. By using linear approximation (1.16), the data complexity of linear cryptanalysis is about 2^{62}, the time complexity is about 2^{55}, 2^{58} and 2^{53} respectively for 128-bit, 192-bit and 256-bit key. So NUSH with 256-bit key is less secure than NUSH with 192-bit key.

1.3.3 Linear cryptanalysis by 28-round linear approximation. By applying eqs. (1.5), (1.8) and (1.10), we see the following 28-round linear approximation which holds with probability $1/2 + 2^{-29}$:

$$f_3(P, KS_0[0—11], KS_1, KS_2, KS_3, KR_0, KR_1, KR_2[0—11]) \oplus 1$$
$$= f_5(M_0[0—9], M_1[0—11], M_2[0—9, 12], M_3[0, 1], KF_0[0,1],$$
$$KF_1[0—9, 12], KF_2[0—11], KF_3[0—9], KR_{32}[0],$$
$$KR_{33}[0], KR_{34}[0], KR_{35}[0—9]). \quad (1.17)$$

By using linear approximation (1.17), the data complexity of attack is about 2^{58}, the time complexity is about 2^{124}, 2^{157} and 2^{125} respectively for 128-bit, 192-bit and 256-bit key.

2 NUSH with 128-bit block

2.1 Relationship among middle value and plaintext and key

As discussed above, $a_1[0] \oplus b_1[0] \oplus d_1[0]$ depends on plaintext, $KS_0[0]$, $KS_1[0—7]$, $KS_2[0—7]$, $KS_3[0]$ and $KR_0[0—7]$. The relationship among them is expressed by function g_1:

$$a_1[0] \oplus b_1[0] \oplus d_1[0]$$
$$= g_1(P, KS_0[0], KS_1[0—7], KS_2[0—7], KS_3[0], KR_0[0—7]). \quad (2.1)$$

Similarly, $a_2[0] \oplus b_2[0] \oplus d_2[0]$ depends on plaintext, $KS_0[0]$, $KS_1[0—12]$, $KS_2[0—12]$, $KS_3[0—5]$, $KR_0[0—12]$ and $KR_1[0—5]$. The relationship among them is expressed by function g_2:

$$\begin{aligned} & a_2[0] \oplus b_2[0] \oplus d_2[0] \\ = & g_2(P, KS_0[0], KS_1[0—12], KS_2[0—12], KS_3[0—5], KR_0[0—12], KR_1[0—5]). \end{aligned} \tag{2.2}$$

Similarly, $a_3[0] \oplus b_3[0] \oplus d_3[0]$ depends on plaintext, $KS_0[0—15]$, $KS_1[0—27]$, $KS_2[0—27]$, $KS_3[0—20]$, $KR_0[0—27]$, $KR_1[0—20]$ and $KR_2[0—15]$. The relationship among them is expressed by function g_3:

$$\begin{aligned} a_3[0] \oplus b_3[0] \oplus c_3[0] = & g_3(P, KS_0[0—15], KS_1[0—27], \\ & KS_2[0—27], KR_3[0—20], KR_0[0—27], KR_1[0—20], KR_2[0—15]). \end{aligned} \tag{2.3}$$

2.2 Relationship among middle value and ciphertext and key

As discussed above, $a_{63}[0] \oplus b_{63}[0] \oplus d_{63}[0]$ depends on ciphertext M, $KF_0[0—14]$, $KF_1[0—4, 17]$, $KF_2[0—14, 20—24]$, $KF_3[0—14]$, $KR_{64}[0]$, $KR_{65}[0]$, $KR_{66}[0]$ and $KR_{67}[0—4]$. The relationship among them is expressed by function g_4:

$$\begin{aligned} a_{63}[0] \oplus b_{63}[0] \oplus d_{63}[0] = & g_4(M, KF_0[0—14], KF_1[0—4, 17], \\ & KF_2[0—14, 20—24], KF_3[0—14], KR_{64}[0], \\ & KR_{65}[0], KR_{66}[0], KR_{67}[0—4]). \end{aligned} \tag{2.4}$$

2.3 Linear cryptanalysis to NUSH with 128-bit block

2.3.1 Linear cryptanalysis by 60-round linear approximation. By applying eqs. (1.5), (2.3) and (2.4), we see the following 60-round linear approximation which holds with probability $1/2 + 2^{-61}$:

$$\begin{aligned} & g_3(P, KS_0[0—15], KS_1[0—27], KS_2[0—27], KS_3[0—20], \\ & KR_0[0—27], KR_1[0—20], KR_2[0—15]) \\ = & g_4(M, KF_0[0—14], KF_1[0—4,17], KF_2[0—14, 20—24], KF_3[0—14], \\ & KR_{64}[0], KR_{65}[0], KR_{66}[0], KR_{67}[0—4]). \end{aligned} \tag{2.5}$$

By using eq.(2.5) to attack NUSH with 128-bit block, the data complexity is about 2^{122}, the time complexity is about 2^{95}, 2^{142} and 2^{168} respectively for 128-bit, 192-bit and 256-bit key.

2.3.2 Linear cryptanalysis by 61-round linear approximation. By applying eqs. (1.5), (2.2) and (2.4), we see the following 61-round linear approximation which holds with probability $1/2 + 2^{-62}$:

$$\begin{aligned} & g_2(P, KS_0[0], KS_1[0—12], KS_2[0—12], KS_3[0—5], \\ & KR_0[0—12], KR_1[0—5]) \\ = & g_4(M, KF_0[0—14], KF_1[0—4,17], KF_2[0—14, 20—24], KF_3[0—14], \\ & KR_{64}[0], KR_{65}[0], KR_{66}[0], KR_{67}[0—4]) \oplus 1. \end{aligned} \tag{2.6}$$

By using eq. (2.6) to attack NUSH with 128-bit block, the data complexity is about 2^{124}, the time complexity is about 2^{57}, 2^{75} and 2^{81} respectively for 128-bit, 192-bit and 256-bit key.

2.3.3 Linear cryptanalysis by 62-round linear approximation. By applying eqs. (1.5), (2.1) and (2.4), we see the following 62-round linear approximation which holds with probability $1/2 + 2^{-63}$:

$$g_1(P, KS_0[0], KS_1[0—7], KS_2[0—7], KS_3[0], KR_0[0—7]) = g_4(M, KF_0[0—14], KF_1[0—4,17], KF_2[0—14, 20—24], KF_3[0—14], KR_{64}[0], KR_{65}[0], KR_{66}[0], KR_{67}[0—4]). \quad (2.7)$$

Using eq. (2.7) to attack NUSH with 128-bit block, the data complexity is about 2^{126}, the time complexity is about 2^{52}, 2^{58} and 2^{64} respectively for 128-bit, 192-bit and 256-bit key.

3 NUSH with 256-bit block

3.1 Relationship among middle value and plaintext and key

As discussed above, $a_2[0] \oplus b_2[0] \oplus d_2[0]$ depends on plaintext P, $KS_0[0]$, $KS_1[0—57]$, $KS_2[0—57]$, $KS_3[0—45]$, $KR_0[0—57]$ and $KR_1[0—45]$. The relationship among them is expressed by function h_1:

$$a_2[0] \oplus b_2[0] \oplus d_2[0] = h_1(P, KS_0[0], KS_1[0—57], KS_2[0—57], KS_3[0—45], KR_0[0—57], KR_1[0—45]). \quad (3.1)$$

3.2 Relationship among middle value and ciphertext and key

As discussed above, $a_{128}[0] \oplus b_{128}[0] \oplus d_{128}[0]$ depends on ciphertext M, $KF_0[0—49]$, $KF_1[0—41]$, $KF_2[0—60]$, $KF_3[0—49]$, $KR_{129}[0]$, $KR_{130}[0]$ and $KR_{131}[0—41]$. The relationship among them is expressed by function h_2:

$$a_{128}[0] \oplus b_{128}[0] \oplus d_{128}[0] = h_2(M, KF_0[0—49], KF_1[0—41], KF_2[0—60], KF_3[0—49], KR_{129}[0], KR_{130}[0], KR_{131}[0—41]). \quad (3.2)$$

Similarly, $a_{127}[0] \oplus b_{127}[0] \oplus d_{127}[0]$ depends on ciphertext M, $KF_0[0—51]$, $KF_1[0—58]$, KF_2, $KF_3[0—58]$, $KR_{128}[0]$, $KR_{129}[0]$, $KR_{130}[0]$ and $KR_{131}[0—58]$. The relationship among them is expressed by function h_3:

$$a_{127}[0] \oplus b_{127}[0] \oplus d_{127}[0] = h_3(M, KF_0[0—51], KF_1[0—58], KF_2, KF_3[0—58], KR_{128}[0], KR_{129}[0], KR_{130}[0], KR_{131}[0—58]). \quad (3.3)$$

3.3 Linear cryptanalysis to NUSH with 256-bit block

3.3.1 Linear cryptanalysis by 125-round linear approximation. By applying eqs. (1.5), (3.1) and (3.3), we see the following 125-round linear approximation which holds with probability $1/2 + 2^{-126}$:

$$h_1(P, KS_0[0], KS_1[0—57], KS_2[0—57], KS_3[0—45], KR_0[0—57], KR_1[0—45]) = h_3(M, KF_0[0—51], KF_1[0—58], KF_2, KF_3[0—58], KR_{128}[0], KR_{129}[0], KR_{130}[0], KR_{131}[0—58]) \oplus 1. \quad (3.4)$$

Using eq. (3.4) to attack NUSH with 256-bit block, the data complexity is about 2^{252}, the time complexity is about 2^{122}, 2^{181} and 2^{240} respectively for 128-bit, 192-bit and 256-bit key.

3.3.2 Linear cryptanalysis by 126-round linear approximation. By applying eqs. (1.5), (3.1) and (3.2), we see the following 125-round linear approximation which holds with probability $1/2 + 2^{-127}$:

$$h_1(P, KS_0[0], KS_1[0—57], KS_2[0—57], KS_3[0—45], KR_0[0—57], KR_1[0—45]) = h_2(M, KF_0[0—49], KF_1[0—41], KF_2[0—60], KF_3[0—49], KR_{129}[0], KR_{130}[0], KR_{131}[0—41]) \oplus 1. \quad (3.5)$$

Using eq. (3.5) to attack NUSH with 256-bit block, the data complexity is about 2^{254}, the time complexity is about 2^{119}, 2^{177} and 2^{219} respectively for 128-bit, 192-bit and 256-bit key.

4 Conclusion

NUSH has 36, 68 or 132 rounds depending on the block length, and support 128-bit, 192-bit and 256-bit key size. In this paper NUSH is analyzed by linear cryptanalysis. The complexity δ of the attack consists of data complexity ε and time complexity η, it is marked with $\delta = (\varepsilon, \eta)$. Three linear approximations are used to analyze NUSH with 64-bit block. When $|K| = 128$ bits, the complexities of three attacks are $(2^{58}, 2^{124})$, $(2^{60}, 2^{78})$ and $(2^{62}, 2^{55})$ respectively. When $|K| = 192$ bits, the complexities of three attacks are $(2^{58}, 2^{157})$, $(2^{60}, 2^{96})$ and $(2^{62}, 2^{58})$ respectively. When $|K| = 256$ bits, the complexities of three attacks are $(2^{58}, 2^{125})$, $(2^{60}, 2^{78})$ and $(2^{62}, 2^{53})$ respectively. Three linear approximations are used to analyze NUSH with 128-bit block. When $|K| = 128$ bits, the complexities of three attacks are $(2^{122}, 2^{95})$, $(2^{124}, 2^{57})$ and $(2^{126}, 2^{52})$ respectively When $|K| = 192$ bits, the complexities of three attacks are $(2^{122}, 2^{142})$, $(2^{124}, 2^{75})$ and $(2^{126}, 2^{58})$ respectively. When $|K| = 256$ bits, the complexities of three attacks are $(2^{122}, 2^{168})$, $(2^{124}, 2^{81})$ and $(2^{126}, 2^{64})$ respectively. Two linear approximations are used to analyze NUSH with 256-bit block. When $|K| = 128$ bits, the complexities of two attacks are $(2^{252}, 2^{122})$ and $(2^{254}, 2^{119})$ respectively. When $|K| = 192$ bits, the complexities of two attacks are $(2^{252}, 2^{181})$ and $(2^{254}, 2^{177})$ respectively. When $|K| = 256$ bits, the complexities of two attacks are $(2^{252}, 2^{240})$ and $(2^{254}, 2^{219})$ respectively. These results show that NUSH is not immune to linear cryptanalysis, and longer key cannot enhance the security of NUSH.

Acknowledgements This work was supported by 973 Project (Grant No. G1999035802) and the National Natural Science Foundation of China (Grant No. 19931010).

References

1. Lebedev, A. N., Volchkov, A. A., NUSH, http: //www.cryptonessie.org.
2. Mitsuru Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology-Eurocrypt'93, Berlin: Springer-Verlag, 1993, 386—397.