We describe the procedure of the attacks on reduced-round KETJE MAJOR and compute the time complexity.

6-round attack on instances of 960-bit padding According to parameters set in Table 1, guess the 3 key bits listed, compute cube sums on variables $v_0, ..., v_{31}$, zero cube sums suggest a right key(i.e. 3 guessed key bits in Table 1). It consumes $2^3 \times 2^{32} = 2^{35}$ computations of 6-round initialization of KETJE MAJOR. According to the property of permutation, it is totally symmetric in z-axis. Thus we can obtain corresponding parameters set with any rotation of i-bit ($0 \leq i < 64$) in z-axis. Therefore, 128 key bits can be recovered by 64 iterations for $0 \leq i < 64$, so the time complexity is $64 \times 2^3 \times 2^{32} = 2^{41}$.

Table 1. Parameters set for attack on 6-round KETJE MAJOR

Ordinary Cube Variables
$A[4][1][2] = A[4][4][2] = v_1$, $A[4][1][4] = A[4][4][4] = v_2$, $A[4][1][10] = A[4][4][10] = v_3$, $A[4][1][11] = A[4][4][11] = v_4$, $A[3][0][14] = A[3][3][14] = v_5$, $A[3][0][17] = A[3][3][17] = v_6$, $A[4][1][19] = A[4][4][19] = v_7$, $A[4][1][20] = A[4][4][20] = v_8$, $A[4][1][27] = A[4][4][27] = v_9$, $A[3][0][28] = A[3][3][28] = v_{10}$, $A[4][1][28] = A[4][4][28] = v_{11}$, $A[3][0][33] = A[3][3][33] = v_{12}$, $A[3][0][36] = A[3][3][36] = v_{13}$, $A[3][0][37] = A[3][3][37] = v_{14}$, $A[4][1][38] = A[4][4][38] = v_{15}$, $A[3][0][45] = A[3][3][45] = v_{16}$, $A[4][1][59] = A[4][4][59] = v_{17}$, $A[4][1][60] = A[4][4][60] = v_{18}$, $A[2][2][18] = A[2][4][18] = v_{19}$, $A[2][2][19] = A[2][4][19] = v_{20}$, $A[2][2][51] = A[2][4][51] = v_{21}$, $A[2][2][27] = A[2][4][27] = v_{22}$, $A[2][2][28] = A[2][4][28] = v_{23}$, $A[2][2][52] = A[2][4][52] = v_{24}$, $A[2][2][53] = A[2][4][53] = v_{25}$, $A[2][2][36] = A[2][4][36] = v_{26}$, $A[2][2][37] = A[2][4][37] = v_{27}$, $A[2][2][39] = A[2][4][39] = v_{28}$, $A[2][2][55] = A[2][4][55] = v_{29}$, $A[2][2][60] = A[2][4][60] = v_{30}$, $A[2][2][62] = A[2][4][62] = v_{31}$
Conditional Cube Variables
$A[3][0][0] = A[3][3][0] = v_0$
Bit Condition
$A[3][3][41] = k_1[42] + A[1][0][42] + A[3][0][41] + A[2][2][42] + A[1][3][42] + 1$, $A[4][4][7] = A[3][0][7] + A[0][2][6] + A[3][3][7]$, $A[2][4][31] = k_1[31] + A[1][0][31] + A[3][0][30] + A[1][3][31] + A[3][3][30] + 1$, $A[3][3][8] = A[3][0][8] + A[4][1][8] + A[0][2][7]$, $A[4][4][49] = A[2][1][50] + A[4][1][49] + A[2][2][50] + A[3][3][50] + A[2][4][50]$, $A[2][4][11] = A[2][1][11] + A[3][3][11] + 1$, $A[2][4][61] = A[2][1][61] + A[2][2][61] + A[3][3][61]$, $A[0][2][38] = k_0[30] + k_1[38] + A[2][1][37] + 1$, $A[4][4][12] = A[2][1][13] + A[4][1][12] + A[3][3][13] + A[2][4][13]$
Guessed Key Bits
$k_1[42], k_1[31], k_0[30] + k_1[38]$

7-round attack on instances of 768-bit padding According to parameters set in Table 2, guess the 16 key bits listed, compute cube sums on variables

$v_0, ..., v_{63}$, zero cube sums suggest a right key(i.e. 16 guessed key bits in Table 2). It consumes $2^{16} \times 2^{64} = 2^{80}$ computations of 7-round initialization of KETJE MAJOR. Similar to the case above, 46 key bits can be recovered by 4 iterations for $0 \leq i < 4$, and the remaining 82 key bits can be recovered by exhaustive search. The time complexity is $4 \times 2^{16} \times 2^{64} + 2^{82} = 2^{83}$.

Table 2. Parameters set for attack on 7-round Ketje Major

Ordinary Cube Variables
$A[3][2][0]=A[3][3][0]=v_1$,$A[1][0][1]=A[1][3][1]=v_2$,$A[4][1][4]=A[4][4][4]=v_3$,
$A[3][0][5]=v_4$,$A[3][2][5]=v_5$,$A[3][3][5]=v_4+v_5$,$A[1][0][7]=A[1][3][7]=v_6$,
$A[1][0][9]=A[1][3][9]=v_7$,$A[3][2][9]=A[3][3][9]=v_8$,$A[4][1][9]=A[4][4][9]=v_9$,
$A[3][0][10]=v_{10}$,$A[3][2][10]=v_{11}$,$A[3][3][10]=v_{10}+v_{11}$,$A[4][1][10]=A[4][4][10]=v_{12}$,
$A[3][2][11]=A[3][3][11]=v_{13}$,$A[4][1][11]=A[4][4][11]=v_{14}$,$A[1][0][12]=A[1][3][12]=v_{15}$,
$A[3][2][15]=A[3][3][15]=v_{16}$,$A[1][0][17]=A[1][3][17]=v_{17}$,$A[1][0][19]=A[1][3][19]=v_{18}$,
$A[4][1][20]=A[4][4][20]=v_{19}$,$A[4][1][26]=A[4][4][26]=v_{20}$,$A[3][0][27]=A[3][2][27]=v_{21}$,
$A[1][0][29]=A[1][3][29]=v_{22}$,$A[3][2][30]=A[3][3][30]=v_{23}$,$A[3][2][31]=A[3][3][31]=v_{24}$,
$A[1][0][32]=A[1][3][32]=v_{25}$,$A[1][0][33]=A[1][3][33]=v_{26}$,$A[4][1][33]=A[4][4][33]=v_{27}$,
$A[3][0][38]=A[3][2][38]=v_{28}$,$A[1][0][39]=A[1][3][39]=v_{29}$,$A[3][0][41]=A[3][3][41]=v_{30}$,
$A[3][0][42]=A[3][2][42]=v_{31}$,$A[1][0][43]=A[1][3][43]=v_{32}$,$A[3][0][43]=A[3][3][43]=v_{33}$,
$A[3][0][45]=A[3][2][45]=v_{34}$,$A[3][0][46]=v_{35}$,$A[3][2][46]=v_{36}$,$A[3][3][46]=v_{35}+v_{36}$,
$A[3][0][47]=A[3][2][47]=v_{37}$,$A[3][0][48]=A[3][2][48]=v_{38}$,$A[3][0][49]=v_{39}$,
$A[3][2][49]=v_{40}$,$A[3][3][49]=v_{39}+v_{40}$,$A[3][2][50]=A[3][3][50]=v_{41}$,
$A[3][2][51]=A[3][3][51]=v_{42}$,$A[3][2][52]=A[3][3][52]=v_{43}$,$A[4][1][52]=A[4][4][52]=v_{44}$,
$A[3][2][53]=A[3][3][53]=v_{45}$,$A[3][0][56]=v_{46}$,$A[3][2][56]=v_{47}$,$A[3][3][56]=v_{46}+v_{47}$,
$A[3][2][60]=A[3][3][60]=v_{48}$,$A[4][1][61]=A[4][4][61]=v_{49}$,$A[1][0][62]=A[1][3][62]=v_{50}$,
$A[3][2][63]=A[3][3][63]=v_{51}$,$A[2][2][20]=A[2][4][20]=v_{52}$,$A[2][1][26]=A[2][4][26]=v_{53}$,
$A[1][0][4]=A[1][3][4]=v_{54}$,$A[2][2][33]=A[2][4][33]=v_{55}$,$A[2][1][35]=v_{56}$,
$A[2][2][35]=v_{57}$,$A[2][4][35]=v_{56}+v_{57}$,$A[2][1][40]=A[2][2][40]=v_{58}$,
$A[2][1][44]=A[2][2][44]=v_{59}$,$A[2][2][45]=A[2][4][45]=v_{60}$,$A[2][2][54]=A[2][4][54]=v_{61}$,
$A[2][1][23]=A[2][2][23]=v_{62}$,$A[1][0][2]=A[1][3][2]=v_{63}$
Conditional Cube Variables
$A[1][0][0]=A[1][3][0]=v_0$
Bit Condition
$A[4][4][42]=k_1[41] + A[1][0][41] + A[4][1][42] + A[0][2][42] + A[1][3][41] + 1$,
$A[2][4][48]=k_0[38] + k_1[48] + A[1][0][48] + A[1][3][48] + A[0][2][46]$,
$A[4][4][47]=k_1[46] + A[1][0][46] + A[4][1][47] + A[1][3][46]+ 1$,
$A[3][3][58]=k_1[59] + A[1][0][59] + A[3][0][58] + A[2][1][59] + A[3][2][58] + A[1][3][59]$,
$A[3][3][17]=k_0[8] + A[3][0][17] + A[0][2][16]+ A[3][2][17]$,
$A[3][3][26]=k_0[17] + A[3][0][26] + A[0][2][25] + A[3][2][26]$,
$A[3][3][27]=k_0[18] + A[0][2][26]$, $A[3][3][47]=k_0[38] + A[0][2][46]$,
$A[3][3][7]=k_1[8] + A[1][0][8] + A[3][0][7] + A[3][2][7] + A[1][3][8]$,
$A[3][3][48]=k_0[39] + A[0][2][47]$,$A[4][4][44]=A[2][1][45] + A[4][1][44] + A[3][3][45]$,
$A[3][3][55]=k_0[46] + A[3][0][55] + A[0][2][54] + A[3][2][55]$,
$A[4][4][41]=A[2][0][42] + A[2][1][42] + A[4][1][41] + A[3][3][42] + A[2][4][42]$,
$A[4][4][46]=k_1[45] + A[1][0][45] + A[4][1][46]+ A[0][2][46] + A[1][3][45] + 1$,
$A[2][4][52]=k_1[52] + A[1][0][52] + A[3][0][51] + A[1][3][52]$,
$A[0][2][43]=k_0[35] + k_1[43] + A[2][0][42] + A[2][1][42] + A[2][4][42] + 1$,
$A[1][3][61]=k_1[61] + A[1][0][61] + A[3][0][60] + A[2][1][61]$,
$A[0][2][44]=k_1[43] + A[2][1][45] + A[3][3][45] + 1$
Guessed Key Bits
$k_1[41]$,$k_0[38] + k_1[48]$,$k_1[46]$,$k_1[59]$,$k_0[8]$,$k_0[17]$,$k_0[18]$,$k_0[38]$,$k_1[8]$,$k_0[39]$,$k_0[46]$,
$k_1[45]$,$k_1[52]$,$k_0[35] + k_1[43]$,$k_1[61]$,$k_1[43]$