Related-Key Differential Attacks on Cobra-H64 and Cobra-H128

Changhoon Lee[1], Jongsung Kim[2], Jaechul Sung[3], Seokhie Hong[1], Sangjin Lee[1], Dukjae Moon[4]

[1] Center for Information Security Technologies(CIST), Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
{crypto77, hsh, sangjin}@cist.korea.ac.kr
[2] Katholieke Universiteit Leuven, ESAT/SCD-COSIC, Belgium
Kim.Jongsung@esat.kuleuven.be
[3] Department of Mathematics, University of Seoul, 90 Cheonnong Dong, Dongdaemun Gu, Seoul, Korea
jcsung@uos.ac.kr
[4] National Security Research Institute, 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
djmoon@etri.re.kr

Abstract. Cobra-H64 and Cobra-H128, which use data-dependent permutations as a main cryptographic primitive, are 64-bit and 128-bit iterated block ciphers with 128-bit and 256-bit keys, respectively. Since these ciphers use very simple key scheduling and controlled permutation (CP) for fast hardware encryption, they are suitable for wireless communications networks which require high-speed networks. Actually, these ciphers have better hardware performances than other ciphers used in security layers of wireless protocols (Wap, OMA, UMTS, IEEE 802.11 and so on). In this paper, however, we show that Cobra-H64 and Cobra-H128 are vulnerable to related-key differential attacks. We first describe how to construct full-round related-key differential characteristics of Cobra-H64 and Cobra-H128 with high probabilities and then we exploit them to attack full-round Cobra-H64 with a complexity of $2^{15.5}$ and Cobra-H128 with a complexity of 2^{44}.

Keywords : Block Ciphers, Cobra-H64, Cobra-H128, Related-Key Attacks, Data-Dependent Permutations

1 Introduction

Many network applications of encryption require low power devices and fast computation components which imply that the number and complexity of the encryption operations should be kept as simply as possible. Recently, data-dependent permutations (DDP) have been introduced as one of cryptographic primitives suitable to attain such goal and the various DDP-based ciphers have been proposed for hardware implementation with low cost, such as CIKS-1 [16], SPECTR-H64 [2]. Since all of them use very simple key scheduling in order to

Table 1. Summary of our attacks on Cobra-H64 and Cobra-H128

Block Cipher	Number of Rounds	Complexity Data / Time
Cobra-H64	10 (full)	$2^{15.5}$RK-CP / $2^{15.5}$
Cobra-H128	12 (full)	2^{44}RK-CP / 2^{44}

RK-CP: Related-Key Chosen Plaintexts, Time: Encryption units

have no time consuming key preprocessing, they are suitable for the applications of many networks requiring high speed encryption in the case of frequent change of keys. However, the simply designed key scheduling algorithms make to help the cryptanalysts apply related-key attacks to such kinds of block ciphers [12, 13].

Cobra-H64 and Cobra-H128 [17], use the switchable operations to prevent weak keys, are 64-bit and 128-bit block ciphers with simple linear key scheduling algorithms, respectively. These ciphers have better hardware implementations and performances (FPGA and ASIC) than other ciphers used in security layers of most of wireless protocols, WAP, OMA, UMTS, IEEE 802.11 and so on.

In this paper, we first present the structural properties of new CP-boxes used in the round function of Cobra-H64 and Cobra-H128, which allow us to make full-round related-key differential characteristics with high probabilities. Finally, we present two related-key differential attacks on full-round Cobra-H64 and Cobra-H128, which require about $2^{15.5}$ and 2^{44} data and time complexity, respectively. Table 1 summarizes our results.

This paper is organized as follows; In Section 2, we introduce some notations and properties of the used controlled permutations. Section 3 briefly describes two block ciphers, Cobra-H64, Cobra-H128, and their structural properties, and Sections 4 and 5 present related-key differential attacks of Cobra-H64 and Cobra-H128. Finally, we conclude in Section 6.

2 Preliminaries

In this section, we introduce notations used in this paper and some properties of controlled permutations which are the components of Cobra-H64 and Cobra-H128. The following notations are used throughout the paper. Bits will be numbered from left to right, starting with bit 1. If $P = (p_1, p_2, \cdots, p_n)$ then p_1 is the most significant bit and p_n is the least significant bit.

- $e_{i,j}$: A binary string in which the i-th and j-th bits are one and the others are zeroes, e.g., $e_{1,2} = (1, 1, 0, \cdots, 0)$.
- $\oplus$: Bitwise-XOR operation
- $\lll$ ($\ggg$) : Left (Right) cyclic rotation
- $\bigcap$: Logical AND

2.1 Controlled-Permutations

In general, controlled permutation (CP) box used in DDP-based ciphers is defined as follows.

Definition 1. *Let $F(X, V)$ be a function $F : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^n$. F is called a CP-box, if $F(X, V)$ is a bijection for any fixed V.*

We denote the above CP-box $F(X, V)$ by $P_{n/m}$, performing permutations on n-bit binary vectors X depending on some controlling m-bit vector V. The $P_{n/m}$-box is constructed by using elementary switching elements $P_{2/1}$ as elementary building blocks performing controlled transposition of two input bits x_1 and x_2. Here, $P_{2/1}$-box is controlled with one bit v and outputs two bits y_1 and y_2, where $y_1 = x_{1+v}$ and $y_2 = x_{2-v}$, i.e., if $v = 1$, it swaps two input bits otherwise (if $v = 0$), does not.

In other words, $P_{n/m}$-box can be represented as a superposition of the operations performed on bit sets :

$$P_{n/m} = L^{V_1} \circ \pi_1 \circ L^{V_2} \circ \pi_2 \circ \cdots \circ \pi_{s-1} \circ L^{V_s}$$

where L is an active layer composed of $n/2$ $P_{2/1}$ parallel elementary boxes, $V_1, V_2, \cdots V_s$ are controlling vectors of the active layers from 1 to $s = 2m/n$, and $\pi_1, \pi_2, \cdots, \pi_{s-1}$ are fixed permutations (See Fig. 1). Fig. 2 shows structure of the $P_{32/96}$ ($P^{-1}_{32/96}$) and $P_{64/192}$ ($P^{-1}_{64/192}$) used in Cobra-H64 and Cobra-H128. Due to the symmetric structure, the mutual inverses, $P_{n/m}$ and $P^{-1}_{n/m}$, differ only with the distribution of controlling bits over the boxes $P_{2/1}$, e.g., $P^{V}_{32/96}$ and $P^{V'}_{32/96}$ are mutually inverse when $V = (V_1, V_2, \cdots, V_6)$ and $V' = (V_6, V_5, \cdots, V_1)$.

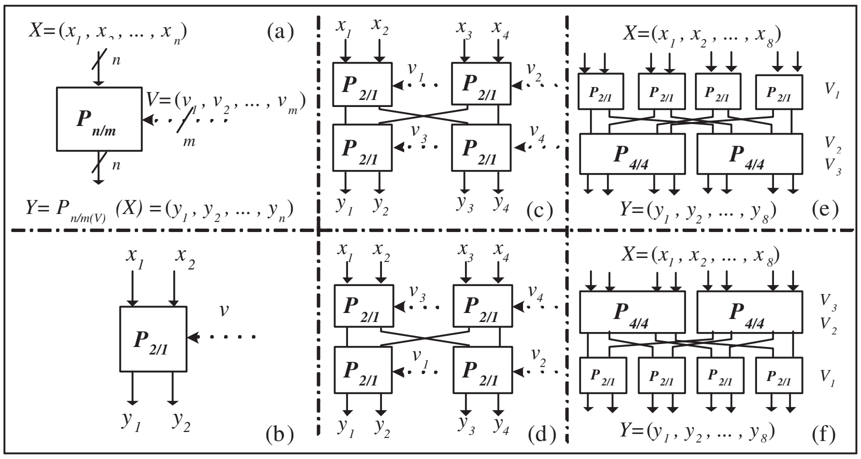

Fig. 1. CP-boxes : (a) $P_{n/m}$, (b) $P_{2/1}$, (c) $P_{4/4}$, (d) $P^{-1}_{4/4}$, (e) $P_{8/12}$, (f) $P^{-1}_{8/12}$

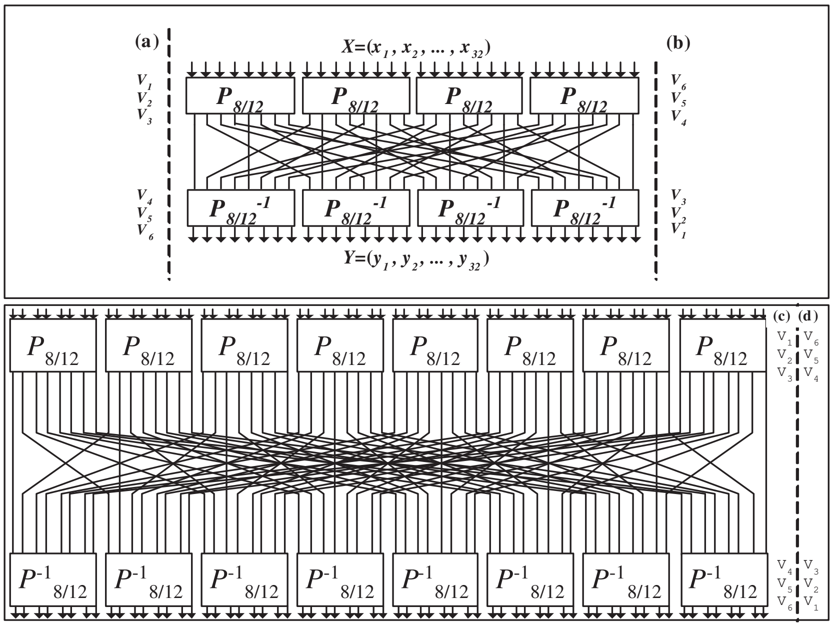

Fig. 2. CP-boxes : (a) $P_{32/96}$, (b) $P_{32/96}^{-1}$, (c) $P_{64/192}$, (d) $P_{64/192}^{-1}$

Now, we present general properties of CP-boxes which can induce properties of operations used in the round function of Cobra-H64 and Cobra-H128.

Property 1. [12,13] Let an input and controlling vector differences of $P_{2/1}$-box be $\Delta X = X \oplus X'$ and $\Delta V = V \oplus V'$ respectively, where X and X' are two-bit input vectors, and V and V' are one-bit controlled vectors. Then we get the following equations.

a) If $\Delta X = 10$(or 01) and $\Delta V = 0$ then the corresponding output difference of $P_{2/1}$-box is $\Delta Y = 10$(or 01) with probability 2^{-1} and $\Delta Y = 01$(or 10) with probability 2^{-1}.
b) If $\Delta X = 00$ and $\Delta V = 1$ then the corresponding output difference of $P_{2/1}$-box is $\Delta Y = 00$ with probability 2^{-1} and $\Delta Y = 11$ with probability 2^{-1}.

The above properties are also expanded into the following properties.

Property 2. [12,13] Let V and V' be m-bit control vectors for $P_{n/m}$-box such that $V \oplus V' = e_i$ $(1 \leq i \leq m)$. Then $P_{n/m(V)}(X) = P_{n/m(V')}(X)$ with probability 2^{-1} where $X \in \{0,1\}^n$. It also holds in $P_{n/m}^{-1}$-box.

Property 3. [12,13] Let X and X' be n-bit inputs for $P_{n/m}$-box such that $X \oplus X' = e_i$ $(1 \leq i \leq n)$. Then $P_{n/m(V)}(X) \oplus P_{n/m(V)}(X') = e_j$ for some j $(1 \leq j \leq n)$.

Property 4. Let $P_{n/m(V)}(X) \oplus P_{n/m(V)}(X \oplus e_i) = e_j$ for some i and j.

a) If $n = 8$, $m = 12$ then the exact one difference route from i to j via three $P_{2/1}$-boxes is fixed. It also holds in $P^{-1}_{8/12}$-box.
b) If $n = 32$, $m = 96$ then the exact two difference routes from i to j via six $P_{2/1}$-boxes are fixed. It also holds in $P^{-1}_{32/96}$-box.
c) If $n = 64$, $m = 192$ then the exact one difference route from i to j via six $P_{2/1}$-boxes is fixed. It also holds in $P^{-1}_{64/192}$-box.

For example, consider $i = 8$ and $j = 2$ in the *Property* 4-a). Then, we can exactly know the 3 bits of control vectors (1,1,0) corresponding to three elements $P_{2/1}$-boxes of $P_{8/12}$-box with probability 1. See Fig. 3. In Fig. 3, the bold line denotes the possible difference route when the input and output differences of $P_{8/12}$ and $P^{-1}_{8/12}$ are fixed.

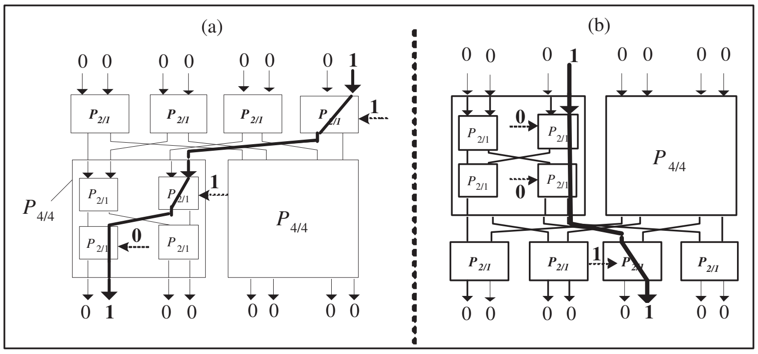

Fig. 3. An example of the difference routes when the input and output differences of $P_{8/12}$ and $P^{-1}_{8/12}$ are fixed.

3 Cobra-H64 and Cobra-H128

In this section, we briefly describe two block ciphers, Cobra-H64, Cobra-H128 [17] and introduce their properties used in our attacks. These ciphers use same iterative structure and are composed of the initial transformation (IT), e-dependent round function $Crypt^{(e)}$, and the final transformation (FT) where $e = 0$ ($e = 1$) denotes encryption (decryption) as follow:

1. An input data block is divided into two subblocks L and R.
2. Perform initial transformation :
   $L_0 = L \oplus O_3$ and $R_0 = R \oplus O_4$, where O_3 and O_4 are subkeys;

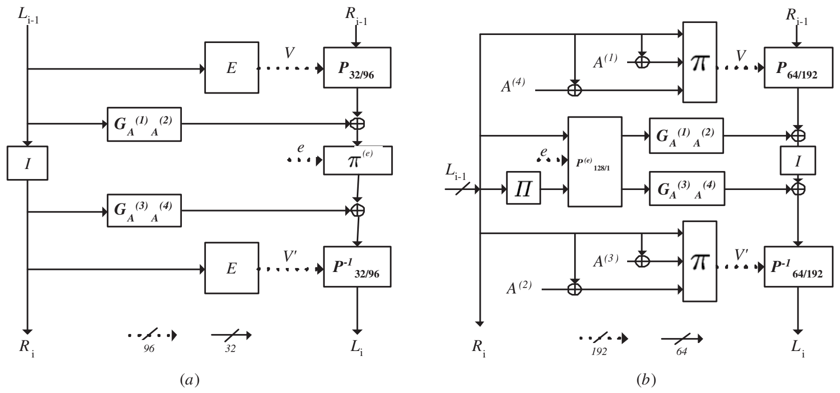

Fig. 4. (a) $Crypt^{(e)}$ of Cobra-H64, (b) $Crypt^{(e)}$ of Cobra-H128

3. For $j = 1$ to $r - 1$ do :
   - $(L_j, R_j) := Crypt^{(e)}(L_{j-1}, R_{j-1}, Q_j^{(e)})$, where $Q_j^{(e)}$ is the j-th round key;
   - Swap the data subblocks : $T = R_j$, $R_j = L_j$, $L_j = T$;
4. $j = r$ do :
   - $(L_r, R_r) := Crypt^{(e)}(L_{r-1}, R_{r-1}, Q_r^{(e)})$;
5. Perform final transformation :
   $C_L = L_r \oplus O_1$ and $C_R = R_r \oplus O_2$, where O_1 and O_2 are subkeys;
6. Return the ciphertext block $C = (C_L, C_R)$.

3.1 A Description of Cobra-H64

Cobra-H64 encrypts 64-bit data blocks with a 128-bit key by iterating a round function 10 times. The $Crypt^{(e)}$ used in Cobra-H64 consists of an extension box E, a switchable fixed permutation $\pi^{(e)}$, a permutational involution I, a nonlinear operation G, and two CP-boxes $P_{32/96}$, $P^{-1}_{32/96}$. See Fig. 4. The extension box E provides the following relation between its input $L = (l_1, \cdots, l_{32})$ and output $V = (V_1, \cdots, V_6)$:

$$V_1 = L_l,\ V_2 = L_l^{\lll 6},\ V_3 = L_l^{\lll 12},\ V_4 = L_h,\ V_5 = L_h^{\lll 6},\ V_6 = L_r^{\lll 12}$$

where $L_l = (l_1, \cdots, l_{16})$, $L_h = (l_{17}, \cdots, l_{32})$, $|l_i| = 1$ $(1 \le i \le 32)$ and $|V_i| = 16$ $(1 \le i \le 6)$.

The switchable fixed permutation $\pi^{(e)}$ performs permutation $\pi^{(0)}$ when enciphering, and $\pi^{(1)}$ when deciphering. Both of them contain two cycles. The first cycle corresponds to identical permutation of the least significant input bit x_{32}. The second cycle is described by the following equations:

$$\pi^{(0)}(x_1, x_2, \cdots, x_{31}) = (x_1, x_2, \cdots, x_{31})^{\lll 5},\ \pi^{(1)}(x_1, x_2, \cdots, x_{31}) = (x_1, x_2, \cdots, x_{31})^{\lll 26}$$

The permutational involution I which is used to strengthen the avalanche effect is performed as follows:

$$I = (1,17)(2,21)(3,25)(4,29)(5,18)(6,22)(7,26)(8,30)(9,19)(10,23) \\ (11,27)(12,31)(13,20)(14,24)(15,28)(16,32).$$

The operation $G_{A'A''}(L)$, which is only nonlinear part in Cobra-H64, is described by the following expression $((A', A'')$ can be round keys $(A^{(1)}, A^{(2)})$ or $(A^{(3)}, A^{(4)}))$:

$$W = L_0 \oplus A_0' \oplus (L_2 \cap L_3) \oplus (L_1 \cap L_2) \oplus (L_1 \cap L_3) \oplus (L_2 \cap A_1'') \oplus (A_1' \cap L_3) \oplus (A_0'' \cap L_1 \cap L_2)$$

where binary vectors L_j, A_j', and A_j'' are expressed as follows:

$$L_0 = L = (l_1, l_2, \cdots, l_{32}), L_1 = (1, l_1, l_2, \cdots, l_{31}), L_2 = (1, 1, l_1, \cdots, l_{30}),$$
$$L_3 = (1, 1, 1, l_1, \cdots, l_{29}), A_0' = A' = (a_1', a_2', \cdots, a_{32}'), A_1' = (1, a_1', a_2', \cdots, a_{31}')$$
$$A_0'' = A'' = (a_1'', a_2'', \cdots, a_{32}''), A_1'' = (1, a_1'', a_2'', \cdots, a_{31}''), A_2'' = (1, 1, a_1'', \cdots, a_{30}'')$$

The key schedule of Cobra-H64 is very simple. An 128-bit master key K is split into four 32-bit blocks, i.e., $K = (K_1, K_2, K_3, K_4)$. Then, in order to generate 10 e-dependent round keys $Q_j^{(e)} = (A_j^{(1)}, A_j^{(2)}, A_j^{(3)}, A_j^{(4)})$ $(1 \le j \le 10)$, K_1,K_2,K_3 and K_4 are rearranged as specified in Table 2 in which $O_i = K_i$ if $e = 0$, $O_1 = K_3$, $O_2 = K_4$, $O_3 = K_1$, $O_4 = K_2$ if $e = 1$.

Table 2. Key schedule of Cobra-H64

j	1	2	3	4	5	6	7	8	9	10
$A^{(1)}_j$	O_1	O_4	O_3	O_2	O_1	O_1	O_2	O_3	O_4	O_1
$A^{(2)}_j$	O_2	O_1	O_4	O_3	O_4	O_4	O_3	O_4	O_1	O_2
$A^{(3)}_j$	O_3	O_2	O_1	O_4	O_3	O_3	O_4	O_1	O_2	O_3
$A^{(4)}_j$	O_4	O_3	O_2	O_1	O_2	O_2	O_1	O_2	O_3	O_4

3.2 A Description of Cobra-H128

Cobra-H128 is a 128-bit block cipher with a 256-bit key and the number of 12 rounds. The $Crypt^{(e)}$ of Cobra-H128 uses two fixed permutations π, Π, a permutational involution I, a nonlinear operation G, and two CP-boxes $P_{64/192}^{(V)}$, $(P_{64/192}^{-1})^{(V')}$ (See Fig. 4). These components are a little bit different from those of Cobra-H64.

1. The permutation Π contains four cycles of the length 16 represented as follows;

   (1,50,9,42,17,34,25,26,33,18,41,10,49,2,57,58)(3,64,43,24,19,48,59,8,35,32,11,56,51,16,27,40)
   (4,7,28,47,52,23,12,63,36,39,60,15,20,55,44,31)(5,14,13,6,21,62,29,54,37,46,45,38,53,30,61,22).

2. π forms the control vectors V and V' using three 64-bit input values for the $P_{64/192}$ and $P^{-1}_{64/192}$-box respectively. For example, let us consider formation of the vector V=$(V_1, V_2, V_3, V_4, V_5, V_6)$=$\pi(L,A_1,A_4)$ where $V_i \in \{0, 1\}^{32}$ and $L,A_1,A_4 \in \{0, 1\}^{64}$ $(1 \le i \le 32)$. Table 3 depicts the distribution of the 192 controlling bits in $P_{64/192}$-box.

V	$P_{64/192}$																														
V_1	31	32	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2
V_2	10'	24'	25'	26'	29'	13'	27'	16'	1'	2'	31'	32'	3'	4'	19'	6'	7'	8'	9'	23'	11'	12'	28'	15'	14'	30'	17'	18'	5'	20'	21'	22'
V_3	13"	14"	15"	16"	17"	18"	19"	20"	21"	22"	23"	24"	25"	26"	27"	28"	29"	30"	31"	32"	1"	2"	3"	4"	5"	6"	7"	8"	12"	10"	11"	9"
V_4	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
V_5	55'	56'	57'	58'	59'	60'	61'	62'	63'	64'	33'	34'	35'	36'	37'	38'	39'	40'	41'	42'	43'	44'	45'	46'	47'	48'	49'	50'	51'	52'	53'	54'
V_6	45"	46"	47"	48"	49"	50"	51"	52"	53"	54"	55"	56"	57"	58"	59"	60"	61"	62"	63"	64"	33"	34"	35"	36"	37"	38"	39"	40"	41"	42"	43"	44"

Table 3. 192 bits control vector V and the corresponding positions for $P_{64/192}$-box

   In Table 3, (V_1,V_4), (V_2,V_5) and (V_3,V_6) are represented as respective rearrangement of bits of L=$(l_1, l_2, \cdots, l_{64})$, $L \oplus A_1$=$(l_1 \oplus a^1_1, l_2 \oplus a^1_2, \cdots, l_{64} \oplus a^1_{64})$ and $L \oplus A_4$=$(l_1 \oplus a^4_1, l_2 \oplus a^4_2, \cdots, l_{64} \oplus a^4_{64})$, i.e., i=l_i, j'=$l_j \oplus a^1_j$ and k''=$l_k \oplus a^4_k$ where $l_i, a^1_j, a^4_k \in \{0, 1\}$ and $1 \le i, j, k \le 64$.

3. I is a permutational involution. It is described as follows:
   $Y = (Y_1, Y_2, \cdots, Y_8) = I(X_1, X_2, \cdots, X_8)$, where $Y_1 = X_6^{\lll 4}$,$Y_2 = X_5^{\lll 4}$, $Y_3 = X_4^{\lll 4}$, $Y_4 = X_3^{\lll 4}$,$Y_5 = X_2^{\lll 4}$,$Y_6 = X_1^{\lll 4}$,$Y_7 = X_8^{\lll 4}$,$Y_8 = X_7^{\lll 4}$ $(1 \le i \le 8)$.

4. G is the only non-linear part of $Crypt^{(e)}$. If L=$(l_1, \ldots, l_{64})$ is a 64-bit input value, and A'=$(a'_1, \ldots, a'_{64})$ and A''=$(a''_1, \ldots, a''_{64})$ are 64-bit subkeys of G then the output value W=$G(L, A', A'')$=$G_{(A',A'')}(L)$ of G is computed as follows;

$$W = L_0 \oplus A'_0 \oplus (L_1 \cap A''_0) \oplus (L_2 \cap L_5) \oplus (L_6 \cap A'_1) \oplus (A''_1 \cap A'_2) \oplus (L_4 \cap L_3) \oplus (L_1 \cap L_6 \cap L_4) \oplus (L_2 \cap L_6 \cap A''_1) \oplus (L_1 \cap A''_1 \cap L_2 \cap L_4),$$

   where $\forall i \in \{0, 1, 2\}$, $\forall j \in \{0, 1, ..., 6\}$, the binary vectors L_j and A_i are defined as : $L_j = L^{\lll 64-j}$, $A_0 = A$, $A_1 = (1, a_1, ..., a_{63})$, $A_2 = (1, 1, a_1, ..., a_{62})$, ($A$=$A'$ or A'').

The key schedule of Cobra-H128 is also very simple and uses Table 4 as a rearrangement of the master key sequences (K_1, K_2, K_3 K_4) where $|K_i|$=64.

Table 4. Key schedule of Cobra-H128

j	1	2	3	4	5	6	7	8	9	10	11	12
$A^{(1)}_j$	O_1	O_4	O_3	O_2	O_1	O_3	O_3	O_1	O_2	O_3	O_4	O_1
$A^{(2)}_j$	O_2	O_3	O_4	O_1	O_2	O_4	O_4	O_2	O_1	O_4	O_3	O_2
$A^{(3)}_j$	O_3	O_2	O_1	O_4	O_3	O_1	O_1	O_3	O_4	O_1	O_2	O_3
$A^{(4)}_j$	O_4	O_1	O_2	O_3	O_4	O_2	O_2	O_4	O_3	O_2	O_1	O_4

3.3 Properties of Cobra-H64 and Cobra-H128

In this subsection, we describe some properties for components of $Crypt^{(e)}$ of Cobra-H64 and Cobra-H128, which allow us to construct strong related key differential characteristics.

Property 5. This is a property for components of $Crypt^{(e)}$ of Cobra-H64.

a) If L is a random input and A', A'' are two random round keys then $G_{A'A''}(L) \oplus G_{A'\oplus e_{32}A''\oplus e_{32}}(L) = 0$ with probability 1/4 (i.e., it holds only when $(l_{30}, l_{31}) = (1,1)$) and $G_{A'A''}(L) \oplus G_{A'\oplus e_{32}A''\oplus e_{32}}(L) = e_{32}$ with probability 3/4 (i.e., it holds only when $(l_{30}, l_{31}) = (0,0), (0,1)$ or $(1,0)$).

b) For any fixed i, j $(1 \le i, j \le 32)$ $\Delta P_{32/96(\Delta V=0)}(\Delta X = e_i) = e_j$ with probability 2^{-5}. (For any fixed i, j there can be two difference routes in $P_{32/96(V)}(X)$, and each route occurs with probability 2^{-6}.) Similarly, it also holds in $P^{-1}_{32/96}$.

Property 6. This is a property for components of $Crypt^{(e)}$ of Cobra-H128.

a) For the control vector V of $P_{64/192}$-box, $\pi(L, A', A'') \oplus \pi(L, A' \oplus e_{64}, A'') = e_{138}$ and $\pi(L, A', A'') \oplus \pi(L, A', A'' \oplus e_{64}) = e_{180}$. For the control vector V' of $P^{-1}_{64/192}$-box, $\pi(L, A', A'') \oplus \pi(L, A' \oplus e_{64}, A'') = e_{42}$ and $\pi(L, A', A'') \oplus \pi(L, A', A'' \oplus e_{64}) = e_{20}$. where $L, A', A'' \in \{0,1\}^{64}$ and $V, V' \in \{0,1\}^{192}$.

b) If L is a random input and A', A'' are two random round keys then $G_{A'A''}(L) \oplus G_{A'\oplus e_{64}A''\oplus e_{64}}(L) = 0$ with probability 1/2 (i.e., it holds only when $l_{63} = 1$) and $G_{A'A''}(L) \oplus G_{A'\oplus e_{64}A''\oplus e_{64}}(L) = e_{64}$ with probability 1/2 (i.e., it holds only when $l_{63} = 0$).

c) For any fixed i, j $(1 \le i, j \le 64)$ $\Delta P_{64/192(\Delta V=0)}(\Delta X = e_i) = e_j$ with probability 2^{-6}. (For any fixed i, j there can be one difference route in $P_{64/192(V)}(X)$, and this route occurs with probability 2^{-6}.) Similarly, it also holds in $P^{-1}_{64/192}$.

4 Related-Key Differential Characteristics on Cobra-H64 and Cobra-H128

In this section, we construct related-key differential characteristics for Cobra-H64 and Cobra-H128 using the properties mentioned in the previous subsection.

4.1 Related-Key Differential Characteristic on Cobra-H64

As stated earlier, the key schedule of the Cobra-H64 is very simple, i.e., the round keys are only 32-bit parts of the 128-bit master key, and there are many useful properties of $P_{32/96}$ and $P_{32/96}^{-1}$ which allow us to construct useful related-key differential characteristics.

In this subsection, we show how to construct full-round (10 rounds) related-key differential characteristics with a high probability. We consider the situation that we encrypt plaintexts $P = (P_L, P_R)$ and $P' = (P'_L, P'_R)$ under an unknown key K=(K_1, K_2, K_3, K_4) and an unknown related-key $K' = (K'_1, K'_2, K'_3, K'_4)$ such that $P \oplus P' = (e_{32}, e_{32})$ and $K \oplus K' = (e_{32}, e_{32}, e_{32}, e_{32})$, respectively. Then we can obtain 32 desired full-round related-key differential characteristics $\alpha \rightarrow \beta_j$ with the same probability of $2^{-12.5}$, where $\alpha = (e_{32}, e_{32})$ and $\beta_j = (e_{32}, e_{j,32})$ for each j $(1 \leq j \leq 32)$ as depicted in Table 5.

Table 5. Related-Key Differential Characteristic of Cobra-H64

Round (i)	ΔRI^i	ΔRK^i	Prob.
IT	(e_{32}, e_{32})	(e_{32}, e_{32})	1
1	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
2	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
3	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
4	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
5	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
6	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
7	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
8	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
9	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16
10	$(0, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	$(3/8) \cdot 2^{-5}$
FT	$(0, e_j)$	(e_{32}, e_{32})	1
Output	$(e_{32}, e_{j,32})$	$\cdot$	$\cdot$
Total	$\cdot$	$\cdot$	$2^{-12.5}$

$1 \leq j \leq 32$: fixed value, if $j = 32$, $e_{j,32} = 0$

The related-key differential characteristics described in Table 5 exploits one round iterative differential characteristic whose input and output differences are $(0, 0)$ and key difference is $(e_{32}, e_{32}, e_{32}, e_{32})$. This one round iterative differential characteristic holds with probability 10/16, which can be obtained as follows.

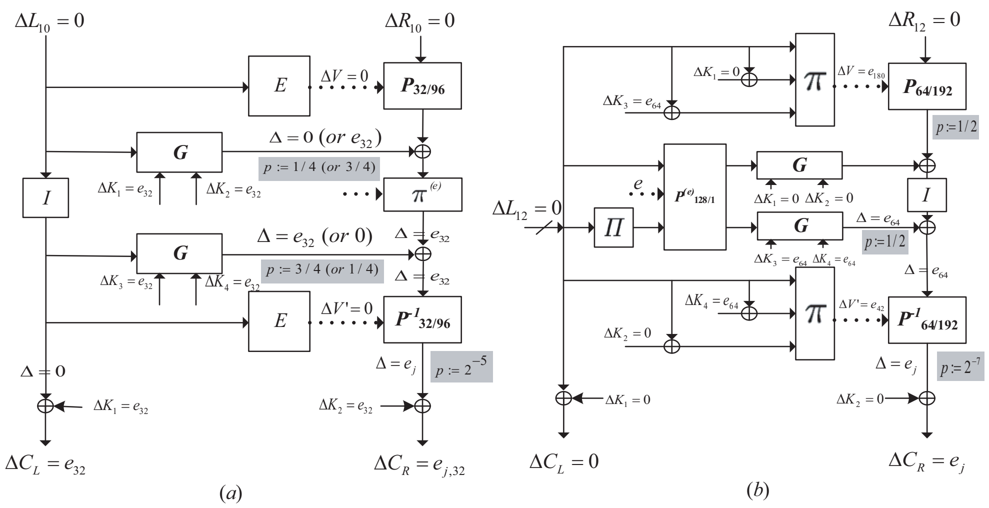

Fig. 5. Propagation of the difference in the last round

Since the $\pi^{(e)}$ function does not affect the least significant bit (i.e., 32-*th* bit), if the output differences of the first and second G functions are both 0 or e_{32} then the one round iterative differential characteristic should be satisfied. According to *Property* 5-a), the output differences of the first and second G functions are both 0 with probability $1/16(= 1/4 \cdot 1/4)$ and the output differences of the first and second G functions are both e_{32} with probability $9/16(= 3/4 \cdot 3/4)$ and thus the one round iterative differential characteristic holds with probability $10/16$.

In order to make a key recovery attack of Cobra-H64 easily, we use another differential characteristic in the last round whose input difference is $(0, 0)$, output difference is $(0, e_j)$ and key difference is $(e_{32}, e_{32}, e_{32}, e_{32})$. This one round differential characteristic holds with probability $(3/8) \cdot 2^{-5}$, which can be obtained as follows. For getting the desired output difference it should be satisfied that one of output differences of the first and second G functions is e_{32} and the other is 0. According to *Property* 5-a), this event occurs with probability $3/8(= 2 \cdot (1/4) \cdot (3/4))$. Since for any fixed j $(1 \leq j \leq 32)$ $\Delta P^{-1}_{32/96(\Delta V=0)}(\Delta X = e_{32}) = e_j$ with probability 2^{-5} (refer to *Property* 5-b)), the last round differential characteristic holds with probability $(3/8) \cdot 2^{-5}$.

In order to verify these results we performed a series of simulations with randomly chosen 2^{14} plaintexts and randomly chosen 3000 related key pairs, respectively. As a result, we checked that there exist more than 3 pairs on average satisfying each of ciphertext differences in Table 5. Our simulation result is higher than our expectation $2^{1.5}(= 2^{14} \times 2^{-12.5})$. This difference is due to the fact that our estimation only considers one differential characteristic rather than a differential.

4.2 Related-Key Differential Characteristic on Cobra-H128

Using the same method presented in the previous subsection, we construct full-round related-key differential characteristics for Cobra-H128. We consider the situation that we encrypt plaintexts P and P' under an unknown key K and an unknown related-key K' such that $P \oplus P' = (e_{64}, e_{64})$ and $K \oplus K' = (0, 0, e_{64}, e_{64})$, respectively. Then we can obtain 64 desired full-round related-key differential characteristics $(e_{64}, e_{64}) \rightarrow (0, e_j)$ $(1 \leq j \leq 64)$ with the same probability of 2^{-42}, as depicted in Table 6.

Since we consider a related-key pair (K, K') satisfying $K \oplus K' = (0, 0, e_{64}, e_{64})$, we know the difference form of each round key is satisfied with $RK = (0, 0, e_{64}, e_{64})$ or $RK = (e_{64}, e_{64}, 0, 0)$ (See Table. 4). Now, according to the condition of RK, we describe one round differential characteristic of $Crypt^{(e)}$ used in our attack.

C1: $RK = (0, 0, e_{64}, e_{64})$

If the input difference of $Crypt^{(e)}$ is zero then, by *Property* 6-*a*), the output difference of the first π is (e_{180}) with probability 1. Thus, by *Property* 2, the output difference of $P_{64/192}$ is zero with probability $P1 = 2^{-1}$ because the input and controlled vector differences are 0 and e_{180}, respectively. Since the input and round key differences of the second G are 0 and (e_{64}, e_{64}), respectively, the corresponding output difference of the second G is 0 with probability $P2 = 2^{-1}$. Similarly, the output difference of the second π is e_{42} and the output difference of $P^{-1}_{64/192}$ is 0 with probability $P3 = 2^{-1}$. Hence if the input difference of $Crypt^{(e)}$ is 0 under $RK = (0, 0, e_{64}, e_{64})$ then the corresponding output difference of $Crypt^{(e)}$ is 0 with probability 2^{-3}.

C2: $RK = (e_{64}, e_{64}, 0, 0)$

If the input difference of $Crypt^{(e)}$ is zero then, by *Property* 6-*a*), the output difference of the first π is (e_{138}) with probability 1. Thus, by *Property* 2, the output difference of $P_{64/192}$ is zero with probability $P1 = 2^{-1}$ because the input and controlled vector differences are 0 and e_{138}, respectively. Since the input and round key differences of the first G are 0 and (e_{64}, e_{64}), respectively, the corresponding output difference of the second G is 0 with probability $P2 = 2^{-1}$. Similarly, the output difference of the second π is e_{20} and the output difference of $P^{-1}_{64/192}$ is 0 with probability $P3 = 2^{-1}$. Hence if the input difference of $Crypt^{(e)}$ is 0 under $RK = (e_{64}, e_{64}, 0, 0)$ then the corresponding output difference of $Crypt^{(e)}$ is 0 with probability 2^{-3}.

We alternatively use *C1* and *C2* to construct the first 11 rounds of our differential characteristics (See Table 6). In the last round, however, we use a little bit different characteristic from *C1* and *C2* for our key recovery attack. In Table 6, the case of *C1'* means that the output difference of the second G in the last round is not zero but e_{64} with probability 2^{-1}, and then by *Property* 2 and *Property* 6-*c*) we have $P3 = 2^{-7}$ in the last round. See Fig. 5.

Table 6. Related-Key Differential Characteristic of Cobra-H128

Round (i)	ΔRI^i	ΔRK^i	$P1/P2/P3$	Prob.	Case
IT	(e_{64}, e_{64})	(e_{64}, e_{64})	$\cdot$	1	$\cdot$
1	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C1*
2	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
3	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
4	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C1*
5	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C1*
6	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
7	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
8	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C1*
9	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C1*
10	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
11	$(0, 0)$	$(e_{64}, e_{64}, 0, 0)$	$2^{-1}/2^{-1}/2^{-1}$	2^{-3}	*C2*
12	$(0, 0)$	$(0, 0, e_{64}, e_{64})$	$2^{-1}/2^{-1}/2^{-7}$	2^{-9}	*C1'*
FT	$(0, e_j)$	$(0, 0)$	$\cdot$	1	$\cdot$
Output	$(0, e_j)$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
Total	$\cdot$	$\cdot$	$\cdot$	2^{-42}	$\cdot$

$1 \leq j \leq 64$: fixed value

5 Key Recovery Attacks on Cobra-H64 and Cobra-H128

We now present key recovery attacks on Cobra-H64 and Cobra-H128 using our related-key differential characteristics.

5.1 Attack Procedure on Cobra-H64

To begin with, we encrypt $2^{14.5}$ plaintext pairs $P = (P_L, P_R)$ and $P' = (P_L \oplus e_{32}, P_R \oplus e_{32})$ under an unknown key $K = (K_1, K_2, K_3, K_4)$ and an unknown related-key $K' = (K_1 \oplus e_{32}, K_2 \oplus e_{32}, K_3 \oplus e_{32}, K_4 \oplus e_{32})$, respectively, and then get the $2^{14.5}$ corresponding ciphertext pairs $C = (C_L, C_R)$ and $C' = (C'_L, C'_R)$, i.e., $E_K(P) = C$ and $E_{K'}(P') = C'$, where E is the block cipher Cobra-H64. Since our full-round related-key differential characteristic of Cobra-H64 has a probability of $2^{-12.5}$, we expect about four ciphertext pair (C, C') such that $C \oplus C' = (e_{32}, e_{j,32})$ for each j $(1 \leq j \leq 32)$. According to our differential trail described in Table 5, we can deduce that the j-th one-bit difference in such (C, C') is derived from the output difference of $P_{2/1}^{({V_6}'^{16})}$ in $P_{32/96}^{-1}$ of the last round (Refer to Fig 6). That is, we can expect that there are two differential routes: one is from $P_{2/1}^{({V_6}'^{16})}$ and $P_{2/1}^{({V_5}'^{14})}$, and the other is from $P_{2/1}^{({V_6}'^{16})}$ and $P_{2/1}^{({V_5}'^{16})}$ (the second one is described in Fig. 6). From each of these two routes, we can extract 6 bits of control vectors by using Property 3. However, since in the attack procedure one route is a right route and the other is a wrong route, one of the two extracted 6 bits may not be correct.

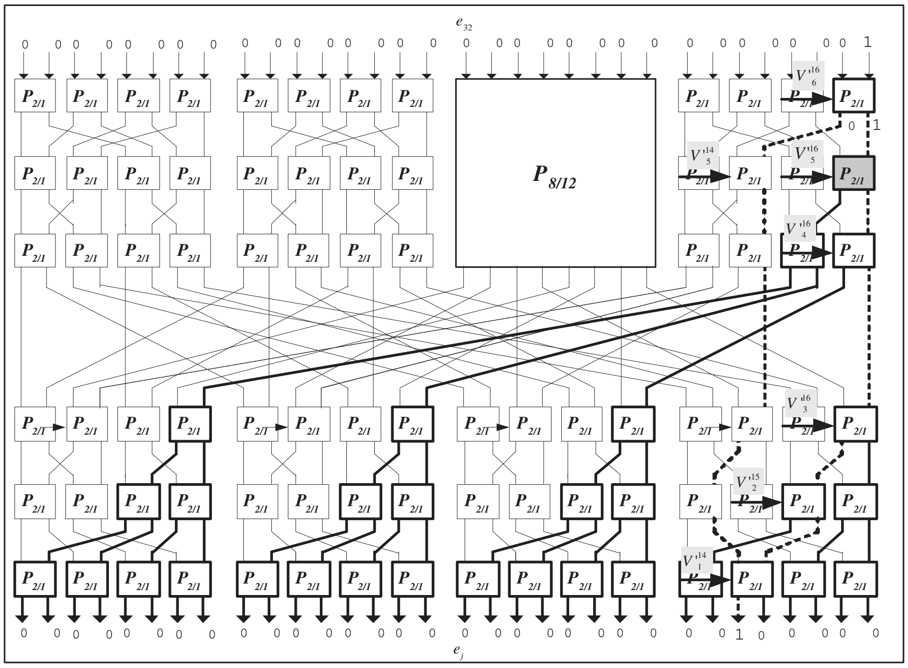

Fig. 6. The possible routes of the non-zero output difference of $P_{2/1}^{(V'^{16}_6)}$-box in $P^{-1}_{32/96}$

For example, assume that output difference is e_{27}. Then we have the following two 6 bits of control vectors (Refer to Fig. 6 and Table 7, 8).

- $v_{96} = C_L^{28} \oplus K_1^{28} = 0$, $v_{80} = C_L^{22} \oplus K_1^{22} = 0$, $v_{64} = C_L^{32} \oplus K_1^{32} = 0$, $v_{48} = C_L^{12} \oplus K_1^{12} = 1$, $v_{31} = C_L^{5} \oplus K_1^{5} = 0$, $v_{14} = C_L^{14} \oplus K_1^{14} = 1$
- $v_{96} = C_L^{28} \oplus K_1^{28} = 1$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0$, $v_{62} = C_L^{30} \oplus K_1^{30} = 0$, $v_{46} = C_L^{10} \oplus K_1^{10} = 1$, $v_{29} = C_L^{3} \oplus K_1^{3} = 0$, $v_{14} = C_L^{14} \oplus K_1^{14} = 0$

From this procedure we can increase counters of extracted keys. If we use enough plaintext pairs to follow the above procedure, we can distinguish the right key from wrong keys by the maximum likelihood method. Based on this idea we can devise a related-key differential attack on full-round Cobra-H64.

1. Prepare $2^{14.5}$ plaintext pairs (P_i, P'_i), $i = 1, \cdots, 2^{14.5}$, which have the (e_{32}, e_{32}) difference. All P_i are encrypted using a master key K and all P'_i are encrypted using a master key K' where K and K' have the $(e_{32}, e_{32}, e_{32}, e_{32})$ difference. Encrypt each plaintext pair (P_i, P'_i) to get the corresponding ciphertext pair (C_i, C'_i).
2. Check that $C_i \oplus C'_i = (e_{32}, e_{j,32})$ for each i and j. We call the bit position of j whose values are 1 OBP(One Bit Position).

3. For each ciphertext pair (C_i, C_i') passing Step 2, extract two 6 bits of control vectors by chasing two difference routes between the OBP and the position of the second input bit in $P_{2/1}^{(V_6{'}^{16})}$. Compute candidates of the corresponding bits of K_1 and K_1' by using Tables 7, 8. Output each 6-bit subkey pair with maximal number of hits (here, each of 6-bit subkey pairs corresponds to one of difference routes).

The data complexity of this attack is $2^{15.5}$ related-key chosen plaintexts. The time complexity of Step 1 is $2^{15.5}$ full-round Cobra-H64 encryptions and the time complexity of Steps 2 and 3 is much less than that of Step 1. By our related-key differential characteristic each ciphertext pair can pass Step 2 with probability at least $2^{-12.5}$ and thus the expectation of ciphertext pairs with the $(e_{32}, e_{j,32})$ differences for each j that pass this test is at least 4. This means that the expected number of hits for each 6-bit right key is 4 (Note that the expected number of hits for each 6-bit right key is not 8, since one of two associated difference routes is wrong). On the other hands, the expected number of hits for each 6-bit wrong key is $8 \cdot 2^{-6}$.

Hence we can retrieve 16 bits of keys in the lower layer of $P_{32/96}^{-1}$ and 7 bits of keys in the upper layer of $P_{32/96}^{-1}$ with a data and a time complexity of $2^{15.5}$. Moreover, this attack can be simply extended to retrieve the whole of master key pair (K, K') by performing an exhaustive search for the remaining keys.

5.2 Attack Procedure on Cobra-H128

Unlike the above attack procedure, a related-key attack on Cobra-H128 directly finds some bits of keys by using difference routes.

1. Prepare 2^{43} plaintext pairs (P_i, P_i'), $i = 1, \cdots, 2^{43}$, which have the (e_{64}, e_{64}) difference. All P_i are encrypted using a master key K and all P_i' are encrypted using a master key K' where K and K' have the $(0, 0, e_{64}, e_{64})$ difference. Encrypt each plaintext pair (P_i, P_i') to get the corresponding ciphertext pair (C_i, C_i').
2. Check that $C_i \oplus C_i' = (0, e_j)$ for each i and j $(1 \leq j \leq 64)$.
3. For each ciphertext pair (C_i, C_i') passing Step 2, extract some bits of control vector by chasing a difference route between this OBP and the position of the 64-*th* input bit in $P_{64/192}^{-1}$ (See Fig. 7). Then find the corresponding bits of K_1, $K_1 \oplus K_2$, and $K_1 \oplus K_3$. Note that the controlled vector V' of $P_{64/192}^{-1}$ in the last round is formatted with $C_L \oplus K_1$, $C_L \oplus K_1 \oplus K_2$, and $C_L \oplus K_1 \oplus K_3$.

The data complexity of this attack is 2^{44} related-key chosen plaintexts. The time complexity of Step 1 is 2^{44} full-round Cobra-H64 encryptions and the time complexity of Steps 2 and 3 is much less than that of Step 1. By our related-key differential characteristics each ciphertext pair can pass Step 2 with probability at least 2^{-42} and thus the expectation of ciphertext pairs with the $(0, e_j)$ difference that pass this test is at least 2. So we have at least one ciphertext

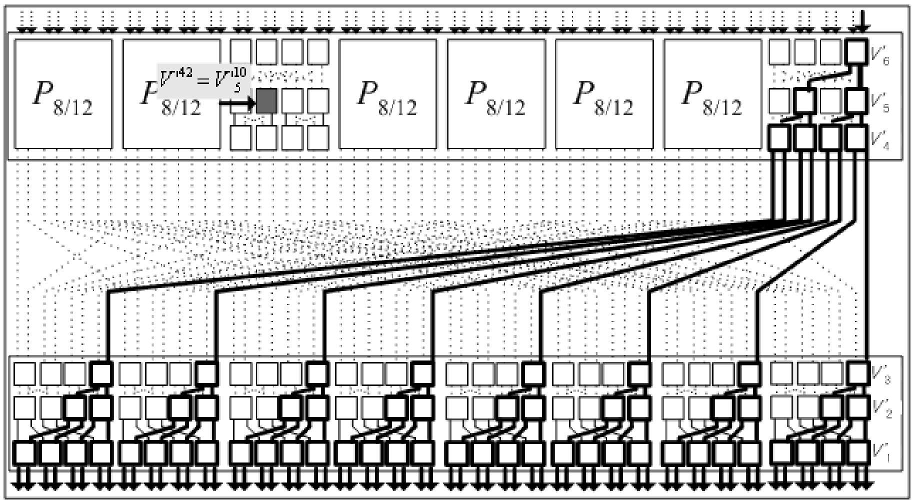

Fig. 7. The possible routes of the 64-th difference of $P^{-1}_{64/192}$

pairs with the $(0, e_j)$ difference for each $1 \leq j \leq 64$. Thus we can retrieve 56 bits of information of keys in the lower layer of $P^{-1}_{64/192}$ and 7 bits of information of keys in the upper layer of $P^{-1}_{64/192}$ with a data and a time complexity of 2^{44}. Similarly, this attack can be simply extended to retrieve the whole of master key pair (K, K') by performing an exhaustive search for the remaining keys.

6 Conclusion

We presented related-key attacks on Cobra-H64 and Cobra-H128. These ciphers are designed suitable for wireless communications networks which require high-speed, but they have a weak diffusion, a weak non-linear operation, and a simple key schedule. So they are vulnerable to related-key differential attacks. According to our results full-round Cobra-H64 can be broken by a complexity of $2^{15.5}$ and full-round Cobra-H128 by a complexity of 2^{44}.

7 Acknowledgments

We would like to thank the anonymous referees and Jesang Lee for helpful comments about this work. This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment). Furthermore, the second author was financed by Ph.D. grants of the Katholieke Universiteit Leuven and of CIST, Korea University and supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT.

References

1. E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer-Verlag, 1993.
2. N. D. Goots, B. V. Izotov, A. A. Moldovyan, and N. A. Moldovyan, "Modern cryptography: Protect Your Data with Fast Block Ciphers", Wayne, A-LIST Publish., 2003.
3. N. D. Goots, B. V. Izotov, A. A. Moldovyan, and N. A. Moldovyan, "Fast Ciphers for Cheap Hardware : Differential Analysis of SPECTR-H64", *MMM-ACNS'03*, LNCS 2776, Springer-Verlag, 2003, pp. 449-452.
4. N. D. Goots, N. A. Moldovyan, P. A. Moldovyanu and D. H. Summerville, "Fast DDP-Based Ciphers: From Hardware to Software", *46th IEEE Midwest International Symposium on Circuits and Systems*, 2003.
5. N. D. Goots, A. A. Moldovyan, N. A. Moldovyan, "Fast Encryption Algorithm Spectr-H64", *MMM-ACNS'01*, LNCS 2052, Springer-Verlag, 2001, pp. 275-286.
6. S. Kavut and M. D. Yücel, "Slide Attack on Spectr-H64", *INDOCRYPT'02*, LNCS 2551, Springer-Verlag, 2002, pp. 34-47.
7. J. Kelsey, B. Schneier, and D. Wagner, "Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES", *Advances in Cryptology - CRYPTO '96*, LNCS 1109, Springer-Verlag, 1996, pp. 237-251.
8. J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", *ICICS'97*, LNCS 1334, Springer-Verlag, 1997, pp. 233-246.
9. J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, "The Related-Key Rectangle Attack - Application to SHACAL-1", *ACISP 2004*, LNCS 3108, Springer-Verlag, 2004, pp. 123-136.
10. J. Kim, G. Kim, S. Lee, J. Lim and J. Song, "Related-Key Attacks on Reduced Rounds of SHACAL-2", *INDOCRYPT 2004*, LNCS 3348, Springer-Verlag, 2004, pp. 175-190.
11. Y. Ko, D. Hong, S. Hong, S. Lee, and J. Lim, "Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property", *MMM-ACNS03*, LNCS 2776, Springer-Verlag, 2003, pp. 298-307.
12. Y. Ko, C. Lee, S. Hong and S. Lee, "Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1 ", *ACISP 2004*, LNCS 3108, 2004, pp. 137-148.
13. Y. Ko, C. Lee, S. Hong, J. Sung and S. Lee, "Related-Key Attacks on DDP based Ciphers: CIKS-128 and CIKS-128H ", *Indocrypt 2004*, LNCS 3348, Springer-Verlag, 2004, pp. 191-205.
14. C. Lee, D. Hong, S. Lee, S. Lee, H. Yang, and J. Lim, "A Chosen Plaintext Linear Attack on Block Cipher CIKS-1", *ICICS 2002*, LNCS 2513, Springer-Verlag, 2002, pp. 456-468.
15. C. Lee, J. Kim, S. Hong, J. Sung, and Sangjin Lee, "Related Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b", *MYCRYPT 2005*, LNCS 3715, Springer-Verlag, 2005, pp. 245-263.

16. A. A. Moldovyan and N. A. Moldovyan, "A cipher Based on Data-Dependent Permutations", *Journal of Cryptology*, volume 15, no. 1 (2002), pp. 61-72
17. N. Sklavos, N. A. Moldovyan, and O. Koufopavlou, "High Speed Networking Security: Design and Implementation of Two New DDP-Based Ciphers", *Mobile Networks and Applications-MONET*, *Kluwer Academic Publishers*, Vol. 25, Issue 1-2, pp. 219-231, 2005.
18. R. C.-W Phan and H. Handschuh, "On Related-Key and Collision Attacks: The case for the IBM 4758 Cryptoprocessor", *ISC 2004*, LNCS 3225, Springer-Verlag, 2004, pp. 111-122.

A Classes of the key bits corresponding to the possible routes

The following two tables represent classes of the key bits corresponding to the possible routes when the non-zero input difference of $P_{2/1}^{(V'^{16}_{6})}$ and output difference e_i in $P^{-1}_{32/96}$-box are fixed

Table 7. Classes of the controlled vectors and key bits corresponding to the possible routes when the non-zero input difference of $P_{2/1}^{(V'^{16}_{5})}$ and output difference e_i in $P^{-1}_{32/96}$-box are fixed.

Class	e_i	Controlled vectors	Key bits
$\mathcal{CL}_1$	e_1	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 1(1)$	K_1^1, K_1^9, K_1^{16}
	(e_2)	$v_{36} = C_L^{16} \oplus K_1^{16} = 1(1),\ v_{19} = C_L^{9} \oplus K_1^{9} = 1(1),\ v_{1} = C_L^{1} \oplus K_1^{1} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_2$	e_3	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 1(1)$	K_1^2, K_1^9, K_1^{16}
	(e_4)	$v_{36} = C_L^{16} \oplus K_1^{16} = 1(1),\ v_{19} = C_L^{9} \oplus K_1^{9} = 0(0),\ v_{2} = C_L^{2} \oplus K_1^{2} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_3$	e_5	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 1(1)$	$K_1^3, K_1^{10}, K_1^{16}$
	(e_6)	$v_{36} = C_L^{16} \oplus K_1^{16} = 0(0),\ v_{20} = C_L^{10} \oplus K_1^{10} = 1(1),\ v_{3} = C_L^{3} \oplus K_1^{3} = 1(0)$	K_1^{22}, K_1^{31}
$\mathcal{CL}_4$	e_7	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 1(1)$	$K_1^4, K_1^{11}, K_1^{16}$
	(e_8)	$v_{36} = C_L^{16} \oplus K_1^{16} = 0(0),\ v_{21} = C_L^{11} \oplus K_1^{11} = 0(0),\ v_{4} = C_L^{4} \oplus K_1^{4} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_5$	e_9	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 0(0)$	K_1^4, K_1^5, K_1^{13}
	(e_{10})	$v_{40} = C_L^{4} \oplus K_1^{4} = 1(1),\ v_{23} = C_L^{13} \oplus K_1^{13} = 1(1),\ v_{5} = C_L^{5} \oplus K_1^{5} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_6$	e_{11}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 0(0)$	K_1^4, K_1^6, K_1^{13}
	(e_{12})	$v_{40} = C_L^{4} \oplus K_1^{4} = 1(1),\ v_{23} = C_L^{13} \oplus K_1^{13} = 0(0),\ v_{6} = C_L^{6} \oplus K_1^{6} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_7$	e_{13}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 0(0)$	K_1^4, K_1^7, K_1^{14}
	(e_{14})	$v_{40} = C_L^{4} \oplus K_1^{4} = 0(0),\ v_{24} = C_L^{14} \oplus K_1^{14} = 1(1),\ v_{7} = C_L^{7} \oplus K_1^{7} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_8$	e_{15}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 1(1),\ v_{63} = C_L^{31} \oplus K_1^{31} = 0(0)$	K_1^4, K_1^8, K_1^{14}
	(e_{16})	$v_{40} = C_L^{4} \oplus K_1^{4} = 0(0),\ v_{24} = C_L^{14} \oplus K_1^{14} = 0(0),\ v_{8} = C_L^{8} \oplus K_1^{8} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{31}$
$\mathcal{CL}_9$	e_{17}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 1(1)$	K_1^1, K_1^8, K_1^{9}
	(e_{18})	$v_{44} = C_L^{8} \oplus K_1^{8} = 1(1),\ v_{27} = C_L^{1} \oplus K_1^{1} = 1(1),\ v_{9} = C_L^{9} \oplus K_1^{9} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{10}$	e_{19}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 1(1)$	K_1^1, K_1^8, K_1^{10}
	(e_{20})	$v_{44} = C_L^{8} \oplus K_1^{8} = 1(1),\ v_{27} = C_L^{1} \oplus K_1^{1} = 0(0),\ v_{10} = C_L^{10} \oplus K_1^{10} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{11}$	e_{21}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 1(1)$	K_1^2, K_1^8, K_1^{11}
	(e_{22})	$v_{44} = C_L^{8} \oplus K_1^{8} = 0(0),\ v_{28} = C_L^{2} \oplus K_1^{2} = 1(1),\ v_{11} = C_L^{11} \oplus K_1^{11} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{12}$	e_{23}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 1(1)$	K_1^2, K_1^8, K_1^{12}
	(e_{24})	$v_{44} = C_L^{8} \oplus K_1^{8} = 0(0),\ v_{28} = C_L^{2} \oplus K_1^{2} = 0(0),\ v_{12} = C_L^{12} \oplus K_1^{12} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{13}$	e_{25}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 0(0)$	$K_1^5, K_1^{12}, K_1^{13}$
	(e_{26})	$v_{48} = C_L^{12} \oplus K_1^{12} = 1(1),\ v_{31} = C_L^{5} \oplus K_1^{5} = 1(1),\ v_{13} = C_L^{13} \oplus K_1^{13} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{14}$	e_{27}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 0(0)$	$K_1^5, K_1^{12}, K_1^{14}$
	(e_{28})	$v_{48} = C_L^{12} \oplus K_1^{12} = 1(1),\ v_{31} = C_L^{5} \oplus K_1^{5} = 0(0),\ v_{14} = C_L^{14} \oplus K_1^{14} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{15}$	e_{29}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 0(0)$	$K_1^6, K_1^{12}, K_1^{15}$
	(e_{30})	$v_{48} = C_L^{12} \oplus K_1^{12} = 0(0),\ v_{32} = C_L^{6} \oplus K_1^{6} = 1(1),\ v_{15} = C_L^{15} \oplus K_1^{15} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$
$\mathcal{CL}_{16}$	e_{31}	$v_{96} = C_L^{28} \oplus K_1^{28} = 0(0),\ v_{80} = C_L^{22} \oplus K_1^{22} = 0(0),\ v_{64} = C_L^{32} \oplus K_1^{32} = 0(0)$	$K_1^6, K_1^{12}, K_1^{16}$
	(e_{32})	$v_{48} = C_L^{12} \oplus K_1^{12} = 0(0),\ v_{32} = C_L^{6} \oplus K_1^{6} = 0(0),\ v_{16} = C_L^{16} \oplus K_1^{16} = 1(0)$	$K_1^{22}, K_1^{28}, K_1^{32}$

Table 8. Classes of the controlled vectors and key bits corresponding to the possible routes when the non-zero input difference of $P_{2/1}^{(V'^{14}_5)}$ and output difference e_i in $P^{-1}_{32/96}$-box are fixed.

Class	e_i	Controlled vectors	Key bits
$\mathcal{CL}_{1'}$	e_1	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 1(1)$	K_1^1, K_1^7, K_1^{14}
	(e_2)	$v_{34} = C_L^{14} \oplus K_1^{14} = 1(1)$, $v_{17} = C_L^7 \oplus K_1^7 = 1(1)$, $v_1 = C_L^1 \oplus K_1^1 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{2'}$	e_3	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 1(1)$	K_1^2, K_1^7, K_1^{14}
	(e_4)	$v_{34} = C_L^{14} \oplus K_1^{14} = 1(1)$, $v_{17} = C_L^7 \oplus K_1^7 = 0(0)$, $v_2 = C_L^2 \oplus K_1^2 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{3'}$	e_5	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 1(1)$	K_1^3, K_1^8, K_1^{14}
	(e_6)	$v_{34} = C_L^{14} \oplus K_1^{14} = 0(0)$, $v_{18} = C_L^8 \oplus K_1^8 = 1(1)$, $v_3 = C_L^3 \oplus K_1^3 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{4'}$	e_7	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 1(1)$	K_1^4, K_1^8, K_1^{14}
	(e_8)	$v_{34} = C_L^{14} \oplus K_1^{14} = 0(0)$, $v_{18} = C_L^8 \oplus K_1^8 = 0(0)$, $v_4 = C_L^4 \oplus K_1^4 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{5'}$	e_9	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 0(0)$	K_1^1, K_1^5, K_1^{11}
	(e_{10})	$v_{38} = C_L^1 \oplus K_1^1 = 1(1)$, $v_{21} = C_L^{11} \oplus K_1^{11} = 1(1)$, $v_5 = C_L^5 \oplus K_1^5 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{6'}$	e_{11}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 0(0)$	K_1^1, K_1^6, K_1^{11}
	(e_{12})	$v_{38} = C_L^1 \oplus K_1^1 = 1(1)$, $v_{21} = C_L^{11} \oplus K_1^{11} = 0(0)$, $v_6 = C_L^6 \oplus K_1^6 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{7'}$	e_{13}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 0(0)$	K_1^1, K_1^7, K_1^{12}
	(e_{14})	$v_{38} = C_L^1 \oplus K_1^1 = 0(0)$, $v_{22} = C_L^{12} \oplus K_1^{12} = 1(1)$, $v_7 = C_L^7 \oplus K_1^7 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{8'}$	e_{15}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 1(1)$, $v_{61} = C_L^{29} \oplus K_1^{29} = 0(0)$	K_1^1, K_1^8, K_1^{12}
	(e_{16})	$v_{38} = C_L^1 \oplus K_1^1 = 0(0)$, $v_{22} = C_L^{12} \oplus K_1^{12} = 0(0)$, $v_8 = C_L^8 \oplus K_1^8 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{29}$
$\mathcal{CL}_{9'}$	e_{17}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 1(1)$	K_1^6, K_1^9, K_1^{15}
	(e_{18})	$v_{42} = C_L^6 \oplus K_1^6 = 1(1)$, $v_{25} = C_L^{15} \oplus K_1^{15} = 1(1)$, $v_9 = C_L^9 \oplus K_1^9 = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{10'}$	e_{19}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 1(1)$	$K_1^6, K_1^{10}, K_1^{15}$
	(e_{20})	$v_{42} = C_L^6 \oplus K_1^6 = 1(1)$, $v_{25} = C_L^{15} \oplus K_1^{15} = 0(0)$, $v_{10} = C_L^{10} \oplus K_1^{10} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{11'}$	e_{21}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 1(1)$	$K_1^6, K_1^{11}, K_1^{16}$
	(e_{22})	$v_{42} = C_L^6 \oplus K_1^6 = 0(0)$, $v_{26} = C_L^{16} \oplus K_1^{16} = 1(1)$, $v_{11} = C_L^{11} \oplus K_1^{11} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{12'}$	e_{23}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 1(1)$	$K_1^6, K_1^{12}, K_1^{16}$
	(e_{24})	$v_{42} = C_L^6 \oplus K_1^6 = 0(0)$, $v_{26} = C_L^{16} \oplus K_1^{16} = 0(0)$, $v_{12} = C_L^{12} \oplus K_1^{12} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{13'}$	e_{25}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 0(0)$	$K_1^3, K_1^{10}, K_1^{13}$
	(e_{26})	$v_{46} = C_L^{10} \oplus K_1^{10} = 1(1)$, $v_{29} = C_L^3 \oplus K_1^3 = 1(1)$, $v_{13} = C_L^{13} \oplus K_1^{13} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{14'}$	e_{27}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 0(0)$	$K_1^3, K_1^{10}, K_1^{14}$
	(e_{28})	$v_{46} = C_L^{10} \oplus K_1^{10} = 1(1)$, $v_{29} = C_L^3 \oplus K_1^3 = 0(0)$, $v_{14} = C_L^{14} \oplus K_1^{14} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{15'}$	e_{29}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 0(0)$	$K_1^4, K_1^{10}, K_1^{15}$
	(e_{30})	$v_{46} = C_L^{10} \oplus K_1^{10} = 0(0)$, $v_{30} = C_L^4 \oplus K_1^4 = 1(1)$, $v_{15} = C_L^{15} \oplus K_1^{15} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$
$\mathcal{CL}_{16'}$	e_{31}	$v_{96} = C_L^{28} \oplus K_1^{28} = 1(1)$, $v_{78} = C_L^{20} \oplus K_1^{20} = 0(0)$, $v_{62} = C_L^{30} \oplus K_1^{30} = 0(0)$	$K_1^4, K_1^{10}, K_1^{16}$
	(e_{32})	$v_{46} = C_L^{10} \oplus K_1^{10} = 0(0)$, $v_{30} = C_L^4 \oplus K_1^4 = 0(0)$, $v_{16} = C_L^{16} \oplus K_1^{16} = 0(1)$	$K_1^{20}, K_1^{28}, K_1^{30}$