# Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b

**Conference Paper** · September 2005
DOI: 10.1007/11554868_18 · Source: DBLP



**5 authors**, including:

Changhoon Lee
Seoul National University of Science and Technology, South Korea
**121** PUBLICATIONS **936** CITATIONS
SEE PROFILE

Jongsung Kim
Kookmin University
**101** PUBLICATIONS **1,571** CITATIONS
SEE PROFILE

Seokhie Hong
Korea University
**178** PUBLICATIONS **1,893** CITATIONS
SEE PROFILE

Jaechul Sung
University of Seoul
**84** PUBLICATIONS **927** CITATIONS
SEE PROFILE

# Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b*

Changhoon Lee[1], Jongsung Kim[2]**, Seokhie Hong[1], Jaechul Sung[3], and Sangjin Lee[1]

[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

**Abstract.** Data-dependent permutations (DDPs) which are very suitable for cheap hardware implementations have been introduced as a cryptographic primitive. Cobra-S128 and Cobra-F64 (which is a generic name for Cobra-F64a and Cobra-F64b) are 128-bit and 64-bit iterated block ciphers with a 128-bit key size based on such DDPs, respectively. Unlike the predecessor DDP-based ciphers [16, 5], Cobra-S128 is a software-oriented cipher and Cobra-F64 is a firmware-suitable cipher. In this paper, we derive several structural properties of Cobra-S128 and Cobra-F64 and then use them to devise key recovery attacks on Cobra-S128 and Cobra-F64. These works are the first known attacks on Cobra-S128 and Cobra-F64.

**Keywords** : Cobra-S128, Cobra-F64, Block Cipher, Related-Key Attack, Data-Dependent Permutation

## 1 Introduction

Recently, data-dependent permutations(DDPs) have been proposed as a cryptographic primitive suitable for cheap hardware implementation. For examples, CIKS-1 [16], SPECTR-H64 [5], and CIKS-128 [2] have been designed based on such DDPs. These ciphers use very simple key scheduling in order to have no time consuming key preprocessing. So, they are suitable for the applications of many network requiring high speed encryption in the case of frequent change

* 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).
** 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

**Table 1.** Summary of our related-key differential attacks

| Block Cipher | Number of Rounds | Complexity Data / Time | Recovered Key Bits |
|---|---|---|---|
| Cobra-S128 (12 rounds) | 12 | $2^{74}$RK-CP / $2^{74}$ | 6 |
| | 12 | $2^{74}$RK-CP / $2^{122}$ | 128(master key) |
| | 12 | $2^{83}$RK-CP / $2^{83}$ | 21 |
| | 12 | $2^{83}$RK-CP / $2^{107}$ | 128(master key) |
| Cobra-F64a (16 rounds) | 11 | $2^{59}$RK-CP / $2^{107}$ | 128(master key) |
| Cobra-F64b (20 rounds) | 18 | $2^{58}$RK-CP / $2^{122}$ | 128(master key) |

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

of keys. Up to now, these ciphers seem to be secure against well known attack methods such as differential cryptanalysis(DC) and linear cryptanalysis(LC) [1, 15, 14, 11, 3]. However, some researchers showed that some DDP-based ciphers with simple key schedules are vulnerable to the related-key attack [12, 13].

Cobra-S128 and Cobra-F64 [4], which use a new DDP and a switchable operation, were proposed to improve the existing DDP-based ciphers. In contrast to the existing DDP-based ciphers which are based on hardware implementation, Cobra-S128 [4] is a 128-bit software-oriented cipher, and Cobra-F64 is a 64-bit firmware-suitable cipher. Note that Cobra-F64 is a generic name for Cobra-F64a and Cobra-F64b.

In this paper, we introduce structural properties for DDP-boxes used in the round function of Cobra-S128 and Cobra-F64, which allow us to make desired related-key differential characteristics. Then, we show how to exploit related-key differential characteristics to devise key recovery attacks on full-round Cobra-S128, 11-round Cobra-F64a and 18-round Cobra-F64b. See Table 1 for our results.

This paper is organized as follows; In Sect. 2, we mention some notations used in this paper and introduce several properties of DDP-boxes. Section 3 briefly describes the Cobra-S128, Cobra-F64 algorithms, and their structural properties, and Section 4 shows our related-key differential characteristics of Cobra-S128, Cobra-F64. We present key recovery attacks of Cobra-S128 and Cobra-F64 in Sect. 5. Section 6 concludes the paper.

## 2 Preliminaries

### 2.1 Notations

For convenience, we use the same notations used in [4]. 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.

- $e_i$ : A binary string in which the $i$-th bit is one and the others are zeroes, e.g., $e_1 = (1, 0, \cdots, 0)$.

– $\oplus$ : Bitwise-XOR operation
– $\boxplus(\boxminus)$ Modulo $2^{32}$ addition(subtraction)
– $\ggg$ : Right cyclic rotation
– $Hw(A)$ : Hamming weight of any binary string $A$

### 2.2 DDP-boxes

In general, DDP-box used in DDP-based ciphers is defined as follows;

**Definition 1.** *Let $F(X,V)$ be the two-variable function such that $F : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$. The function $F(X,V)$ is called a DDP-box, if for each fixed $V$ function $F(X,V)$ is a bijective mapping defined as bit permutation.*

We denote the above DDP-box $F(X,V)$ by $P_{n/m}$ (See Fig. 1). 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 control 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 $P_{32/96}$ and $P^{-1}_{32/96}$ used in Cobra-S128 and Cobra-F64. Due to the symmetric structure, the mutual inverses, $P_{32/96}$ and $P^{-1}_{32/96}$, differ only with the distribution of controlling bits over the boxes $P_{2/1}$, i.e., $P^{V}_{32/96}$ and $P^{V'}_{32/96}$ are mutually inverse when $V = (V_1, V_2, \cdots, V_6)$ and $V' = (V_6, V_5, \cdots, V_1)$.

Now, we introduce some properties of DDP-boxes. We let $x_1x_2$ be a two-bit input string of $P_{2/1}$ and $v$ be an one-bit control vector.

*Property 1.* [12, 13] $P_{2/1(v=0)}(x_1x_2) = P_{2/1(v=1)}(x_1x_2)$ with probability $2^{-1}$.

The equation in the above property holds only when $x_1 = x_2$.

*Property 2.* [12, 13] Let an input and control 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 control vectors. Then we have the following equations.

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

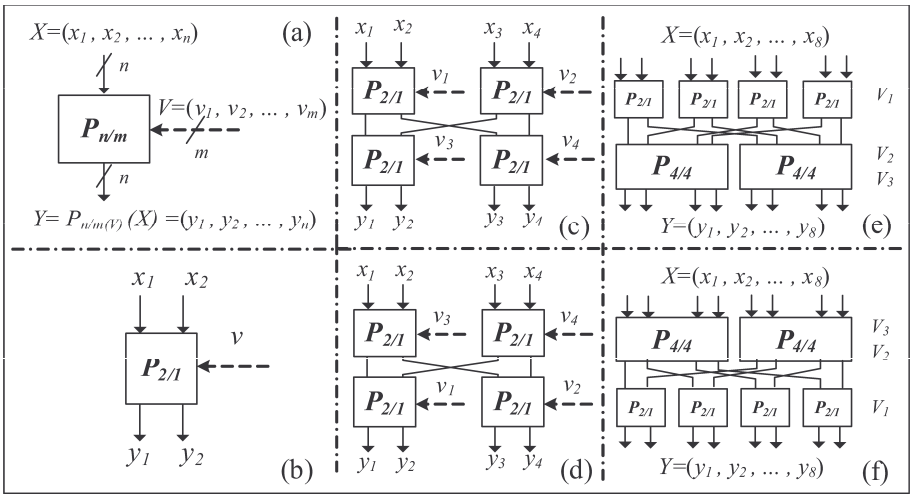


**Fig. 1.** $CP$-boxes : (a) $P_{n/m}$, (b) $P_{2/1}$, (c) $P_{4/4}$, (d) $P^{-1}_{4/4}$, (e) $P_{8/12}$, (f) $P^{-1}_{8/12}$

*c*) If $\Delta X = 00$ and $\Delta V = 1$ such that $X = X' = 10$ or $01$ then the corresponding output difference of $P_{2/1}$-box is $\Delta Y = 11$. Thus, if $\Delta X = 00$ and $\Delta V = 1$ then the corresponding output difference of $P_{2/1}$-box is $\Delta Y = 11$ with probability $2^{-1}$.

The above properties are also expanded into the following properties.

*Property 3.* [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 a probability of $2^{-1}$ where $X \in \{0,1\}^n$. It also holds in $P^{-1}_{n/m}$-box.

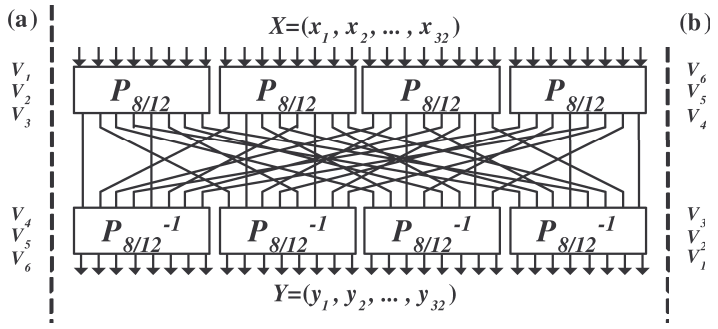


**Fig. 2.** $CP$-boxes : (a) $P_{32/96}$, (b) $P^{-1}_{32/96}$

*Property 4.* [12, 13] If $X \oplus X' = e_i$ $(1 \leq i \leq m)$ then $P_{8/12(V)}(X) \oplus P_{8/12(V)}(X')$ $= e_j$ for some $j$ $(1 \leq j \leq m)$. In addition, if $i$ and $j$ are fixed then the exact difference route from $i$ to $j$ via three $P_{2/1}$-boxes is also fixed. It also holds in $P^{-1}_{8/12}$-box.

For example, consider $i = 4$ and $j = 6$ in the *Property* 4. Then, we can exactly know the 3 bits of control vectors (0,0,1) corresponding to three elements $P_{2/1}$-boxes of $P^{-1}_{8/12}$-box with probability 1. See Fig. 3. In Fig. 3, the bold line denotes the difference route when the input and output differences of $P^{-1}_{8/12}$-box are fixed as $e_4$ and $e_6$, respectively.

*Property 5.* [12, 13] Let $Y = P_{n/m(V)}(X)$ and $Y' = P_{n/m(V)}(X')$. Then $Hw(X \oplus X') = Hw(Y \oplus Y')$. It also holds in $P^{-1}_{n/m}$-box.

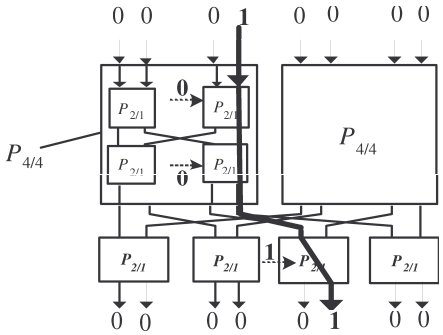


**Fig. 3.** An example of the difference route when the input and output differences of $P^{-1}_{8/12}$-box are fixed as $e_4$ and $e_6$, respectively.

## 3 Cobra-S128 and Cobra-F64

In this section, we briefly describe the block cipher Cobra-S128, Cobra-F64a, and Cobra-F64b [4] and derive their several properties used in our attacks.

### 3.1 Description of Cobra-S128 Cipher

Cobra-S128 is a 128-bit iterated block cipher with a 128-bit key size and 12 rounds. This cipher is composed of the initial transformation, $e$-dependent round function $Crypt^{(e)}$, and the final transformation where $e = 0 (e = 1)$ denotes encryption(decryption). The data encryption procedure is performed as follows. See Fig. 6 in Appendix A.

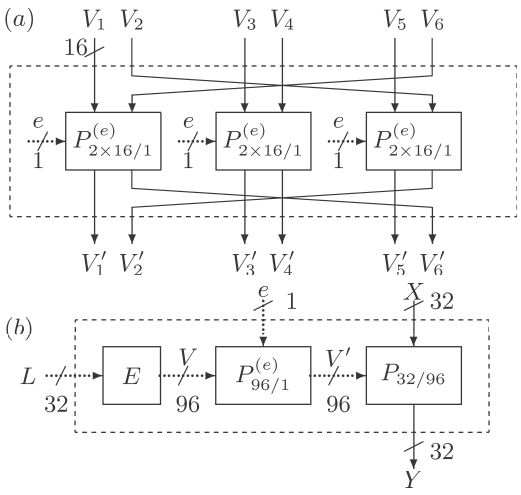


**Fig. 4.** (a) $P^{(e)}_{96/1}$, (b) $P^{(e)}_{32/32}$

1. An 128-bit input data block is divided into four 32-bit subblocks $A$, $B$, $C$, $D$.
2. Perform initial transformation :
   $(A, B, C, D) := (A \oplus Q_1^{(1,e)}, B \oplus Q_2^{(1,e)}, C \oplus Q_3^{(1,e)}, D \oplus Q_4^{(1,e)})$
3. For $j = 1$ to 11 do :
   $(A, B, C, D) := Crypt^{(e)}(A, B, C, D, Q_j^{(1,e)}, Q_j^{(2,e)})$; $(A, B, C, D) := (B, A, D, C)$
4. $j = 12$ do :
   $(A, B, C, D) := Crypt^{(e)}(A, B, C, D, Q_{12}^{(1,e)}, Q_{12}^{(2,e)})$;
5. Perform final transformation :
   $(A, B, C, D) := (A \oplus Q_{12}^{(2,e)}, B \oplus Q_{11}^{(2,e)}, C \oplus Q_{10}^{(2,e)}, D \oplus Q_9^{(2,e)})$
6. Output $(A, B, C, D)$

The $Crypt^{(e)}$ function is composed of the basic arithmetical operations $(\oplus, \boxplus, \boxminus)$ and DDP-box $P_{32/32}$ which is made up of a extension box $E$, a simple transposition box $P^{(e)}_{96/1}$, and $P_{32/96}$ (See Fig. 4). The extension box $E$ provides the following relation between its input $L = (l_1, \cdots, l_{32})$ and output $V = (V_1, \cdots, V_6)$:

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

where $L_l = (l_1, \cdots, l_{16})$, $L_r = (l_{17}, \cdots, l_{32})$, $|l_i| = 1$ $(1 \le i \le 32)$ and $|V_i| = 16$ $(1 \le i \le 6)$. The transposition box $P^{(e)}_{96/1}$ is implemented as some single layer controlled permutation box consisting of three parallel single layer boxes $P^{(e)}_{2\times16/1}$ (See Fig. 4). An input of each $P^{(e)}_{2\times16/1}$-box is divided into 16-bit left and 16-bit right inputs, and contains 16 parallel $P^{(e)}_{2/1}$-boxes controlled with the same bit $e$.

So, if the input vector of the box $P_{96/1}^{(e)}$ is $V = (V_1, \cdots, V_6)$ then the corresponding output vector is $V' = (V_1, \cdots, V_6)$ when $e = 0$ or $V' = (V_6, \cdots, V_1)$ when $e = 1$.

The key schedule of Cobra-S128 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 the subkey sequences $(Q_j^{(1,0)}, Q_j^{(2,0)})$, $K_1$,$K_2$,$K_3$ and $K_4$ are rearranged as specified in Table 2 in which $(Q_j^{(1,0)}, Q_j^{(2,0)})$ denotes the $j$-th round key sequence $(1 \leq j \leq 12)$, and $Q_j^{(1,0)}, Q_j^{(2,0)} \in \{0,1\}^{32}$.

**Table 2.** Key schedule of Cobra-S128, Cobra-F64a, and Cobra-F64b

| $j$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $Q_j^{(1,0)}$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | $K_2$ | $K_1$ | $K_4$ | $K_3$ | $K_1$ | $K_2$ | $K_4$ |
| $Q_j^{(2,0)}$ | $K_4$ | $K_3$ | $K_1$ | $K_2$ | $K_3$ | $K_2$ | $K_1$ | $K_4$ | $K_2$ | $K_3$ | $K_1$ |
| $j$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | . |
| $Q_j^{(1,0)}$ | $K_3$ | $K_1$ | $K_4$ | $K_2$ | $K_3$ | $K_2$ | $K_4$ | $K_3$ | $K_1$ | $K_2$ | . |
| $Q_j^{(2,0)}$ | $K_2$ | $K_3$ | $K_1$ | $K_3$ | $K_4$ | $K_3$ | $K_1$ | $K_4$ | $K_2$ | $K_3$ | . |

### 3.2 Description of Cobra-F64 Ciphers

Cobra-F64a and Cobra-F64b, which are suitable for firmware implementation, are 64-bit iterated block ciphers with a 128-bit key size and 16 and 20 rounds, respectively. These ciphers perform data encryption procedure as follows;

1. 64-bit input data block is divided into two 32-bit subblocks $A$, $B$.
2. For $j = 1$ to $R - 1$ do :
   $(A, B) := Crypt^{(e)}(A, B, Q_j^{(1,e)}, Q_j^{(2,e)})$; $(A, B) := (B, A)$
3. $j = R$ do :
   $(A, B) := Crypt^{(e)}(A, B, Q_j^{(1,e)}, Q_j^{(2,e)})$;
4. Perform final transformation :
   $(A, B) := (A \oplus Q_{R+1}^{(1,e)}, B \oplus Q_{R+1}^{(2,e)})$ for Cobra-F64b and $(A, B) := (A \boxminus Q_{R+1}^{(1,e)}, B \boxplus Q_{R+1}^{(2,e)})$ for Cobra-F64a
5. Output $(A \parallel B)$

   The detailed description for $Crypt^{(e)}$ is presented in Fig. 7 in Appendix A. Cobra-F64a and Cobra-F64b also use Table. 2 as key schedule.

### 3.3 Properties of Cobra-S128 and Cobra-F64

In this subsection, we derive some properties of operations used in round function Cobra-S128 and Cobra-F64 which are useful to construct related-key differential characteristics.

*Property 6.* Let $\Delta X$ and $\Delta V$ be differences of input and control vector of $P_{32/96}$, respectively. Then we can get the following properties of $P_{32/96}$ from the definition of $P_{32/96}$ and the previous properties (*Property* 1,2,3,5).

*a)* $\Delta P_{32/96(\Delta V=0)}(\Delta X = 0) = 0$ with a probability of 1.
*b)* $\Delta P_{32/96(\Delta V=e_1)}(\Delta X = 0) = 0$ with a probability of $2^{-1}$.
*c)* $\Delta P_{32/96(\Delta V=0)}(\Delta X = e_1) = e_1$ with a probability of $2^{-6}$ because $P_{32/96}$ consists of 6 active layers.
*d)* $\Delta P_{32/96(\Delta V=e_1)}(\Delta X = e_1) = e_1$ with a probability of $2^{-6}$ because $P_{32/96}$ consists of 6 active layers.

Similarly, we can also derive the difference property for $P_{32/32}$ as follows.

*Property 7.* Let $\Delta X$ and $\Delta V$ be differences of input and control vector of $P_{32/32}$, respectively. Then the following equations are obtained from the definition of extension box $E$ used in $P_{32/32}$ and the above *Property* 6.

*a)* $\Delta P_{32/32(\Delta L=0)}(\Delta X = 0) = 0$ with probability 1.
*b)* $\Delta P_{32/32(\Delta L=e_1)}(\Delta X = 0) = 0$ with probability $2^{-3}$.
*c)* $\Delta P_{32/32(\Delta L=0)}(\Delta X = e_1) = e_1$ with probability $2^{-6}$.
*d)* $\Delta P_{32/32(\Delta L=e_1)}(\Delta X = e_1) = e_1$ with probability $2^{-8}$.
*e)* $\Delta P_{32/32(\Delta L=e_9)}(\Delta X = e_1) = e_1$ with probability $2^{-9}$.
*f)* $\Delta P_{32/32(\Delta L=e_{1,9})}(\Delta X = e_1) = e_1$ with probability $2^{-11}$.
*g)* $HW(\Delta P_{32/32(\Delta L=e_1)}(\Delta X = 0)) = 0, 2, 4, 6$ by *Property* 2, 5.

## 4 Related-Key Differential Characteristics of Cobra-S128 and Cobra-F64

In this section, we construct related-key differential characteristics for Cobra-S128 and Cobra-F64 using the properties mentioned in the previous subsection.

As stated earlier, the key schedules of the Cobra-S128 and Cobra-F64 are very simple, i.e., the round keys are only 32-bit parts of the 128-bit master key, and there are many properties due to the structural feature of $P_{32/32}$-box. They allow us to construct good related-key differential characteristics even though it uses an $P_{32/32}$-box.

In order to find good related-key differential characteristics, we performed a series of simulations (in which we used a number of plaintext and key differences whose hamming weights are one in each 32-bit word). As our simulation results, we obtained a full-round (12 rounds) related-key differential characteristic $(0, 0, e_1, e_1) \rightarrow (0, 0, 0, t)$ of Cobra-S128 with probability $2^{-72}$, a 12-round related-key differential characteristic $(e_1, e_1) \rightarrow (e_1, t)$ of Cobra-F64a with probability $2^{-62}$, and a full-round (20 rounds) related-key differential characteristic $(0, e_1) \rightarrow (e_1 \oplus t^{\ggg 8}, t)$ of Cobra-F64b with probability $2^{-62}$, where $t$ represents any 32-bit word of which the first byte have hamming weight 1 and the second byte has also hamming weight 1 and the other two bytes has hamming weight 0. Note that these related-key differential characteristics of Cobra-S128,

Cobra-F64a, and Cobra-F64b include their final transformations(FT) and use key differences $(0,0,e_1,0)$, $(0,0,0,e_1)$, and $(e_1,e_1,e_1,e_1)$, respectively. Subsection 4.1 describes our full-round related-key differential characteristic of Cobra-S128 in more detail. See appendix B for the complete forms of characteristics of Cobra-F64a and Cobra-F64b (which can be constructed by the same arguments as in the below subsection). But, in our attacks, we use 11-round related-key differential characteristic of Cobra-F64a and 18-round related-key differential characteristic of Cobra-F64b because the attacks over 11-round Cobra-F64a and 18-round Cobra-F64b lead more complexities than exhaustive search.

### 4.1 How to Construct the Full-Round Related-Key Differential Characteristic of Cobra-S128

In Table 3, $\Delta RI^{I'}$ and $\Delta RK^{I'}$ denote the plaintext and initial key differences, respectively. $\Delta RI^i$ and $\Delta RK^i$ are the input and key differences of $ith$ round, respectively, and ($P1$,$P2$,$P3$,$P4$,$P5$,$P6$) are the respective probabilities that for given input and control vector differences of ($P^{B,e}_{32/32}$, $P^{C,1}_{32/32}$, $P^{C,e}_{32/32}$, $P^{C',e}_{32/32}$, $P^{B,0}_{32/32}$, $P^{B',e}_{32/32}$) boxes used in Cobra-S128, their corresponding output differences satisfy a specific output difference, $e_1$ or 0. These probabilities are obtained from *Property* 6, 7.

Specifically, since the plaintext and initial key differences of Cobra-S128 are $(0,0,e_1,e_1)$ and $(0,0,e_1,0)$ respectively, the input difference of the first round is to be $(0,0,0,e_1)$. Thus the output differences of $P^{B,e}_{32}$ and $P^{C,1}_{32}$ are 0 because the input and control vector differences of $P^{B,e}_{32/32}$ and $P^{C,1}_{32/32}$ are 0. Also, since the input and control vector differences of $P^{C,e}_{32/32}$ are $e_1$ and 0, respectively, the corresponding output difference of $P^{C,e}_{32/32}$ is to be $e_1$ with probability $2^{-6}$ by *Property* 6, 7. Similarly, the output differences of $P^{B,0}_{32}$ and $P^{C',e}_{32}$ are 0 with the probability of 1 because the input and control vector differences of $P^{B,0}_{32/32}$ and $P^{C',e}_{32/32}$ are 0. Furthermore, since the input and control vector differences of $P^{B',e}_{32/32}$ are $e_1$ and 0 in the first round, respectively, the corresponding output difference of $P^{B',e}_{32/32}$ is to be $e_1$ with a probability of $2^{-6}$ by *Property* 6, 7. So, the output difference of the first round is $(0,0,0,e_1)$ with a probability of $2^{-12}$, i.e., the input difference of the second round is $(0,0,e_1,0)$ as mentioned in Table 3. Repeating this manner for the rest of the rounds, we can obtain an output difference $(0,0,0,0)$ after 11 rounds with probability $2^{-66}$ as presented in Table 3.

Proceeding to the last round, since the input and key difference are $(0,0,0,0)$ and $(e_1,0)$, respectively, the input and control vector differences of $P^{(B,0)}_{32/32}$ are 0 and $e_1$, respectively, and thus the corresponding output difference of $P^{(B,0)}_{32/32}$ is to be 0 with probability $2^{-3}$. So, the input and control vector differences of $P^{(B',e)}_{32/32}$ are 0 and $e_1$, respectively. Here, we consider the hamming weight of the

**Table 3.** Related-Key Differential Characteristic of Cobra-S128

| Round ($i$) | $\Delta RI^i$ | $\Delta RK^i$ | $P1/P2/P3/P4/P5/P6$ | Prob. |
|---|---|---|---|---|
| IT | $(0,0,e_1,e_1)$ | $(0,0,e_1,0)$ | $\cdot$ | 1 |
| 1 | $(0,0,0,e_1)$ | $(0,0)$ | $1/1/2^{-6}/1/1/2^{-6}$ | $2^{-12}$ |
| 2 | $(0,0,e_1,0)$ | $(0,e_1)$ | $1/2^{-3}/2^{-3}/1/1/1$ | $2^{-6}$ |
| 3 | $(0,0,0,0)$ | $(e_1,0)$ | $1/1/1/1/2^{-3}/2^{-3}$ | $2^{-6}$ |
| 4 | $(0,0,0,e_1)$ | $(0,0)$ | $1/1/2^{-6}/1/1/2^{-6}$ | $2^{-12}$ |
| 5 | $(0,0,e_1,0)$ | $(0,e_1)$ | $1/2^{-3}/2^{-3}/1/1/1$ | $2^{-6}$ |
| 6 | $(0,0,0,0)$ | $(0,0)$ | $1/1/1/1/1/1$ | 1 |
| 7 | $(0,0,0,0)$ | $(0,0)$ | $1/1/1/1/1/1$ | 1 |
| 8 | $(0,0,0,0)$ | $(e_1,0)$ | $1/1/1/2^{-3}/2^{-3}$ | $2^{-6}$ |
| 9 | $(0,0,0,e_1)$ | $(0,0)$ | $1/1/2^{-6}/1/1/2^{-6}$ | $2^{-12}$ |
| 10 | $(0,0,e_1,0)$ | $(0,e_1)$ | $1/2^{-3}/2^{-3}/1/1/1$ | $2^{-6}$ |
| 11 | $(0,0,0,0)$ | $(0,0)$ | $1/1/1/1/1/1$ | 1 |
| 12 | $(0,0,0,0)$ | $(e_1,0)$ | $1/1/1/1/2^{-3}/2^{-3}$ | $2^{-6}$ |
| FT | $(0,0,e_1,t)$ | $(0,0,e_1,0)$ | $\cdot$ | 1 |
| Output | $(0,0,0,t)$ | $\cdot$ | $\cdot$ | $\cdot$ |
| Total | $\cdot$ | $\cdot$ | $\cdot$ | $2^{-72}$ |

output difference of $P_{32/32}^{(B',e)}$ in the last round in order to construct a related-key differential characteristic suitable for our attack scenario. The hamming weight of the output difference of $P_{32/32}^{(B',e)}$ depends on an input form of $P_{32/96}$ in $P_{32/32}^{B',e}$. Let the control vector of $P_{32/96}$ in $P_{32/32}^{B',e}$ be $V' = (V'_1, V'_2, V'_3, V'_4, V'_5, V'_6)$. Since the control vector difference of $P_{32/32}^{B',e}$ is $e_1$, it is propagated via $E$ into the first bit of $V'_1$, the seventh bit of $V'_2$, and 13th bit of $V'_3$ of $P_{32/96}$. For convenience, we denote three $P_{2/1}$-boxes corresponding to the first bit of $V'_1$, the seventh bit of $V'_2$, and 13th bit of $V'_3$ $P_{2/1}^{V'_{1_1}}$, $P_{2/1}^{V'_{2_7}}$, and $P_{2/1}^{V'_{3_{13}}}$, respectively (See Fig. 5). Note that an input difference of $P_{32/96}$ in $P_{32/32}^{B',e}$ is 0. Then we can classify the input forms of these $P_{2/1}$-boxes corresponding to the above 3 controlled bits into 8 cases. However, in our attack, we consider the hamming weight of the output difference of $P_{32/32}^{(B',e)}$ in the last round is to be 2 under the condition that the form of input pair $(x_1x_2, x'_1x'_2)$ of $P_{2/1}^{V'_{3_{13}}}$ has $(10,10)$ or $(01,01)$, and the input pair of $P_{2/1}^{V'_{1_1}}$ and $P_{2/1}^{V'_{2_7}}$ has any value $(x_1x_2, x'_1x'_2)$ whose difference is zero. Then the output difference of $P_{2/1}^{V'_{3_{13}}}$ has 11 with probability $2^{-1}$ by *Property* 2-*c*), and the output differences of $P_{2/1}^{V'_{1_1}}$ and $P_{2/1}^{V'_{2_7}}$ have 00 with a probability of $2^{-1}$ by *Property* 1, respectively. In more detail, one-bit of two-bit active output differences of $P_{2/1}^{V'_{3_{13}}}$ is propagated into the fourth-bit of the first $P_{8/12}^{-1}$ in $P_{32/96}$ and the other one-bit is propagated into the fourth-bit of the second

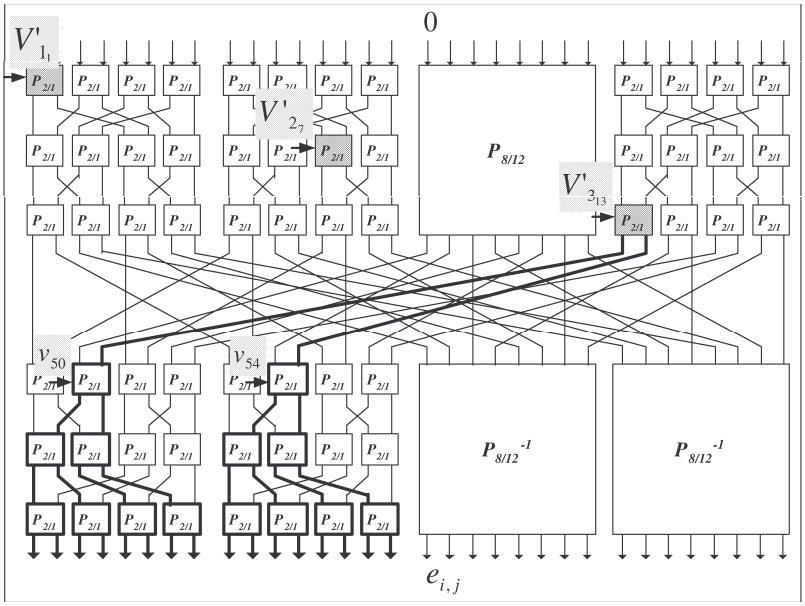


**Fig. 5.** The possible routes of the output difference of $P_{2/1}^{V'_3{}^{13}}$-box in $P_{32/96}$

$P_{8/12}^{-1}$ in $P_{32/96}$ (Refer to Fig. 5). So the resultant probability is $2^{-3}(= P_6)$ that satisfies the first and second output bytes of $P_{32/32}$ having hamming weight 1 and the other bytes having hamming weight 0 by *Property* 5, 7. Hence a full-round related-key differential characteristic $(0, 0, e_1, e_1) \rightarrow (0, 0, 0, t)$ holds with probability $2^{-72}$ when $K \oplus K' = (0, 0, e_1, 0)$.

## 5 Related-Key differential Attacks on Cobra-S128 and Cobra-F64

We now present key recovery attacks on Cobra-S128 and Cobra-F64 using our related-key differential characteristics.

### 5.1 Attack Procedure on Cobra-S128

We first show how to search for a master key pair of Cobra-S128 by using the full-round related-key differential characteristic presented in Section 4. Note that, from the previous full-round related-key differential characteristic, we know that the hamming weight of output difference of $P_{32/32}^{B',e}$ in the last round is 2 (one is in the first $P_{8/12}^{-1}$ and the other is in the second $P_{8/12}^{-1}$) with probability $2^{-72}$.

To begin with, we encrypt $2^{73}$ plaintext pairs $P = (P_{LL}, P_{LR}, P_{RL}, P_{RR})$ and $P' = (P_{LL}, P_{LR}, P_{RL} \oplus e_1, P_{RR} \oplus e_1)$ under an unknown key $K = (K_1, K_2, K_3, K_4)$ and an unknown related-key $K' = (K_1, K_2, K_3 \oplus e_1, K_4)$, respectively, and then get the $2^{73}$ corresponding ciphertext pairs $C = (C_{LL}, C_{LR}, C_{RL}, C_{RR})$ and $C' = (C'_{LL}, C'_{LR}, C'_{RL}, C'_{RR})$, i.e., $E_K(P) = C$ and $E_{K'}(P) = C'$, where $E$ is the block cipher Cobra-S128. Since our full-round related-key differential characteristic of Cobra-S128 has a probability of $2^{-72}$, we expect at least one ciphertext pair $(C, C')$ such that $C \oplus C' = (0, 0, 0, t)$ with a probability of $1-(1-2^{-72})^{2^{73}} \approx 0.87$. According to our differential trail described in Table 3, we can deduce that the two difference bits in such $(C, C')$ are derived from $V'_{3_{13}}$ of the last $P_{32/96}$ (Refer to Fig 5). That is, we can expect that there are two exact routes: One is from the $4th$ bit in input difference of the first $P^{-1}_{8/12}$ to the $ith$ bit of the output difference of the first $P^{-1}_{8/12}$ $(1 \le i \le 8)$ and the other is from the $12th$ bit in input difference of the second $P^{-1}_{8/12}$ to the $ith$ bit of the output difference of the second $P^{-1}_{8/12}$ $(9 \le i \le 16)$. Note that the control vectors and key bits corresponding to the above routes are uniquely determined by Property 4. See Figs. 3 and 5.

**Table 4.** Classes of the control vectors and key bits corresponding to the possible routes when the fourth bit of the first $P^{-1}_{8/12}$ and output difference $e_i$ in $P_{32/96}$-box are fixed.

| Class | $e_i$ | Control vectors | Key bits |
|---|---|---|---|
| $\mathcal{CL}_1$ | $e_1$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 1,\ v_{65} = C^{27}_{RL} \oplus K^{27}_3 = 1,\ v_{81} = C^{21}_{RL} \oplus K^{21}_3 = 0$ | $K^{19}_3, K^{27}_3, K^{21}_3$ |
| | $e_2$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 1,\ v_{65} = C^{27}_{RL} \oplus K^{27}_3 = 1,\ v_{81} = C^{21}_{RL} \oplus K^{21}_3 = 1$ | |
| $\mathcal{CL}_2$ | $e_3$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 1,\ v_{65} = C^{27}_{RL} \oplus K^{27}_3 = 0,\ v_{82} = C^{22}_{RL} \oplus K^{22}_3 = 0$ | $K^{19}_3, K^{27}_3, K^{22}_3$ |
| | $e_4$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 1,\ v_{65} = C^{27}_{RL} \oplus K^{27}_3 = 0,\ v_{82} = C^{22}_{RL} \oplus K^{22}_3 = 1$ | |
| $\mathcal{CL}_3$ | $e_5$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 0,\ v_{66} = C^{28}_{RL} \oplus K^{28}_3 = 1,\ v_{83} = C^{23}_{RL} \oplus K^{23}_3 = 0$ | $K^{19}_3, K^{28}_3, K^{23}_3$ |
| | $e_6$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 0,\ v_{66} = C^{28}_{RL} \oplus K^{28}_3 = 1,\ v_{83} = C^{23}_{RL} \oplus K^{23}_3 = 1$ | |
| $\mathcal{CL}_4$ | $e_7$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 0,\ v_{66} = C^{28}_{RL} \oplus K^{28}_3 = 0,\ v_{84} = C^{24}_{RL} \oplus K^{24}_3 = 0$ | $K^{19}_3, K^{28}_3, K^{24}_3$ |
| | $e_8$ | $v_{50} = C^{19}_{RL} \oplus K^{19}_3 = 0,\ v_{66} = C^{28}_{RL} \oplus K^{28}_3 = 0,\ v_{84} = C^{24}_{RL} \oplus K^{24}_3 = 1$ | |

**Table 5.** Classes of the control vectors and key bits corresponding to the possible routes when the fourth bit of the second $P^{-1}_{8/12}$ and output difference $e_i$ in $P_{32/96}$-box are fixed.

| Class | $e_i$ | Control vectors | Key bits |
|---|---|---|---|
| $\mathcal{CL}_5$ | $e_9$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 1,\ v_{69} = C^{31}_{RL} \oplus K^{31}_3 = 1,\ v_{85} = C^{25}_{RL} \oplus K^{25}_3 = 0$ | $K^{23}_3, K^{31}_3, K^{25}_3$ |
| | $e_{10}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 1,\ v_{69} = C^{31}_{RL} \oplus K^{31}_3 = 1,\ v_{85} = C^{25}_{RL} \oplus K^{25}_3 = 1$ | |
| $\mathcal{CL}_6$ | $e_{11}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 1,\ v_{69} = C^{31}_{RL} \oplus K^{31}_3 = 0,\ v_{86} = C^{26}_{RL} \oplus K^{26}_3 = 0$ | $K^{23}_3, K^{31}_3, K^{26}_3$ |
| | $e_{12}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 1,\ v_{69} = C^{31}_{RL} \oplus K^{31}_3 = 0,\ v_{86} = C^{26}_{RL} \oplus K^{26}_3 = 1$ | |
| $\mathcal{CL}_7$ | $e_{13}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 0,\ v_{70} = C^{32}_{RL} \oplus K^{32}_3 = 1,\ v_{87} = C^{27}_{RL} \oplus K^{27}_3 = 0$ | $K^{23}_3, K^{32}_3, K^{27}_3$ |
| | $e_{14}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 0,\ v_{70} = C^{32}_{RL} \oplus K^{32}_3 = 1,\ v_{87} = C^{27}_{RL} \oplus K^{27}_3 = 1$ | |
| $\mathcal{CL}_8$ | $e_{15}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 0,\ v_{70} = C^{32}_{RL} \oplus K^{32}_3 = 0,\ v_{88} = C^{28}_{RL} \oplus K^{28}_3 = 0$ | $K^{23}_3, K^{32}_3, K^{28}_3$ |
| | $e_{16}$ | $v_{54} = C^{23}_{RL} \oplus K^{23}_3 = 0,\ v_{70} = C^{32}_{RL} \oplus K^{32}_3 = 0,\ v_{88} = C^{28}_{RL} \oplus K^{28}_3 = 1$ | |

Fig. 5 represents the possible routes of the output difference of $P_{2/1}^{V'_{3_{13}}}$-box in $P_{32/96}$ and the bold line denotes a trace of non-zero difference. Tables 4 and 5 represent classes of the control vectors and key bits corresponding to the possible routes when $i$ is fixed. For example, assume that output difference is $e_{1,9}$. Then since the control vectors of three $P_{2/1}$ corresponding to route from the fourth bit of input difference of the first $P_{8/12}^{-1}$ to the first bit of output difference of the first $P_{8/12}^{-1}$ are $v_{50} = C_{RL}^{19} \oplus K_3^{19} = 1$, $v_{65} = C_{RL}^{27} \oplus K_3^{27} = 1$, and $v_{81} = C_{RL}^{21} \oplus K_3^{21} = 0$ where $C^j$ and $K^j$ mean the $j-th$ bits of $C$ and $K$, respectively, we can know three key bits $K_3^{19}$, $K_3^{27}$, and $K_3^{21}$. Similarly, since the control vectors of three $P_{2/1}$ corresponding to route from the fourth bit of input difference of the second $P_{8/12}^{-1}$ to the first bit of output difference of the second $P_{8/12}^{-1}$ are $v_{54} = C_{RL}^{23} \oplus K_3^{23} = 1$, $v_{69} = C_{RL}^{31} \oplus K_3^{31} = 1$, and $v_{85} = C_{RL}^{25} \oplus K_3^{25} = 0$, we can know three key bits $K_3^{23}$, $K_3^{31}$, and $K_3^{25}$. Based on this idea we can devise a related-key differential attack on full-round Cobra-S128 as follows.

1. Prepare $2^{73}$ plaintext pairs $(P_i, P'_i)$, $i = 1, \cdots, 2^{73}$, which have the $(0, 0, e_1, e_1)$ 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 $(0, 0, e_1, 0)$ difference. Encrypt each plaintext pair $(P_i, P'_i)$ to get the corresponding ciphertext pair $(C_i, C'_i)$.
2. Check that $C_i \oplus C'_i = (0, 0, 0, t)$ for each $i$. We call the bit positions of $t$ whose values are 1 BOP(Bit One Position). Note that there are two BOPs.
3. For each ciphertext pair $(C_i, C'_i)$ passing Step 2, extract some bits of control vector by chasing a difference route between the first BOP and the position of the fourth input bit in the first $P_{8/12}^{-1}$ and by chasing a difference route between the second BOP and the position of the fourth input bit of the second $P_{8/12}^{-1}$. Find the corresponding bits of $K_3$ and $K'_3$ by using Tables 4 and 5.

The data complexity of this attack is $2^{74}$ related-key chosen plaintexts. Step 1 is the data collection step and thus this step requires a time complexity of $2^{74}$ encryptions. By our related-key differential characteristic each ciphertext pair can pass Step 2 with probability at least $2^{-72}$ and thus the expectation of ciphertext pairs that pass this test is at least 2. Step 2 can be done efficiently by checking ciphertext differences in byte unit and Step 3 also requires a small amount of time complexity. Furthermore, for each ciphertext pair that passes this test the probability that its difference is derived from the $P_{2/1}^{V'_{1_1}}$ or $P_{2/1}^{V'_{2_7}}$ not $P_{2/1}^{V'_{3_{13}}}$ is less than $2^{-74}$. Hence we can retrieve some portion (at least 6 bits) of subkey matrials by performing Step 3 with high probability. Moreover, if we perform an exhaustive search of the remaining key bits we can find the whole of master key pair $(K, K')$ with a data complexity of $2^{74}$ related-key chosen plaintexts and a time complexity of at most $2^{122}$ encryptions.

From now on, we introduce improved procedure to search for a master key pair, which has a trade-off in data and time complexities. Unlike the above

attack, this attack simultaneously consider three types of ciphertext pairs whose differences have hamming weight 2: the first type is associated with $V'_{3_{13}}$ as like the above attack, the second type is associated with $V'_{2_7}$ and the third type is associated with $V'_{1_1}$. In this attack, we classify these three types of ciphertext pairs into Cases 1, 2, and 3, respectively.

1. Prepare $2^{82}$ plaintext pairs $(P_i, P'_i)$, $i = 1, \cdots, 2^{82}$, which have the same conditions as the above Step 1. Encrypt each plaintext pair $(P_i, P'_i)$ to get the corresponding ciphertext pair $(C_i, C'_i)$.
2. Check that $C_i \oplus C'_i = (0, 0, 0, t')$ for each $i$, where $t'$ is any 32-bit word which has hamming weight 2 such that one is in the first byte and the other is in the second byte (Case 1), or one is in the first byte and the other is in the third byte (Case 2), or one is in the third byte and the other is in the fourth byte (Case 3). We call the bit position which has 1 in $t'$ BOP$'$.
3. For each ciphertext pair $(C_i, C'_i)$ in Case 1, extract the corresponding 3 bits of control vector by chasing a difference route between the first BOP$'$ and the position of the fourth input bit in the first $P^{-1}_{8/12}$ and also extract the corresponding 3 bits of control vector by making a difference route between the second BOP$'$ and the position of the fourth input bit of the second $P^{-1}_{8/12}$. Compute candidates of the corresponding bits of $K_3$ and $K'_3$ by using Tables 4 and 5. Output each 3-bit subkey pair with maximal number of hits (each 3-bit subkey pair corresponds to each difference route).
4. The same arguments can be applied to the Cases 2 and 3. For each ciphertext pair $(C_i, C'_i)$ in Case 2 (resp., Case 3), extract the corresponding 4 (resp., 5) bits of control vector by making a difference route between the first BOP$'$ and the position of the sixth input bit in the first $P^{-1}_{8/12}$ (resp., the position of the first input bit in the third $P^{-1}_{8/12}$) and also extract the corresponding 4 (resp., 5) bits of control vector by making a difference route between the second BOP$'$ and the position of the sixth input bit of the third $P^{-1}_{8/12}$ (resp., the position of the fifth input bit in the fourth $P^{-1}_{8/12}$). Compute candidates of the corresponding bits of $K_3$ and $K'_3$ by using $C_i$, $C'_i$, and extracted control vectors (in Case 2 (resp., Case 3), we can extract some bits of control vectors by making difference routes from the $P_{2/1}$ of $V'_{2_7}$ (resp., $V'_{1_1}$) to BOP$'$s). Output each 4-bit (resp., 5-bit) subkey pair with maximal number of hits in Case 2 (resp., in Case 3).

The data complexity of this attack is $2^{83}$ related-key chosen plaintexts. The probability that a fixed two-bit difference in Case 1 is connected with the $P_{2/1}$ of $V'_{3_{13}}$ is $2^{-6}$ (this probability is derived from *Property* 2-*a*) and *Property* 4) and thus the total probability is $2^{-72-6} = 2^{-78}$. It follows that the expected number of hits for each right 3-bit subkey is about $(2^{-78} \cdot 2^{82})^2 \cdot 16 = 2^{12}$. On the other hands, the probability that a fixed two-bit difference in Case 1 is connected with the $P_{2/1}$ of $V'_{1_1}$ or $V'_{2_7}$ is $2^{-10} \cdot 2 = 2^{-9}$ and thus the expected number of hits for each wrong 3-bit subkey is about $(2^{-72-9} \cdot 2^{82})^2 \cdot 16 \cdot 2^{-3} = 2^3$. This argument can be also applied to Cases 2 and 3. In Case 2, the expected

number of hits for each right 4-bit subkey is about $(2^{-72-8} \cdot 2^{82})^2 \cdot 16 = 2^8$ and in Case 3, the expected number of hits for each right 5-bit subkey is about $(2^{-72-10} \cdot 2^{82})^2 \cdot 16 = 2^4$. Indeed, during the above procedure, subkey candidates can be checked by the overlapped control vectors (this fact makes easy to find the right subkey material). Taking into account these overlapped values, we retrieve 21 bits of the key by this attack. This attack can also retrieve the whole of master key pair $(K, K')$ by performing an exhaustive search for the remaining keys and thus we can find the master key pair with a data complexity of $2^{83}$ related-key chosen plaintexts and a time complexity of $2^{107}$ encryptions.

### 5.2 Attack Procedure on Cobra-F64

Using two attack algorithms presented in previous subsection, we can similarly devise key recovery attacks on 11-round Cobra-F64a and 18-round Cobra-F64b. As for 11 rounds of Cobra-F64a, the above second attack scenario can be efficiently applied with some modifications, and as for 18 rounds of Cobra-F64b, the above first attack scenario can be efficiently applied with some modifications.

Let us first consider 11-round Cobra-F64a. In the second attack scenario, Step 2 collects ciphertext pairs whose differences satisfy $(e_1, t')$ where plaintext pairs have the $(e_1, e_1)$ difference and the master key pair has the $(0, 0, 0, e_1)$ difference. In Steps 3 and 4, for each 32-bit subkey $K_2$ we check the number of ciphertext pairs satisfying $C_i + K_2, C'_i + K_2 \in S(V)$, where $S(V)$ is a set of all 32-bit control vectors such that the control bits extracted by ciphertext pairs $(C_i, C'_i)$ in Cases 1, 2, or 3 are fixed. In this way, we find out a group of 32-bit subkeys $K_2$ with maximal number of hits. With this group, we do an exhaustive search for the remaining 96-bit keys.

In this attack, we use a 11-round related-key differential characteristic $(e_1, e_1) \rightarrow (e_1, t')$ of Cobra-F64a which includes the FT. This characteristic can be derived from Table 6 by cutting off the 12-th round. The probability that $t'$ is in Case 1 whose two BOP′s are specified is about $2^{-48} \cdot 2^{-6} = 2^{-54}$, and the probability that $t'$ is in Case 2 (resp., Case 3) whose two BOP′s are specified is about $2^{-48} \cdot 2^{-8} = 2^{-56}$ (resp., $2^{-48} \cdot 2^{-10} = 2^{-58}$). Thus, if we use $2^{58}$ plaintext pairs, the expected number of hits for the right subkey $K_2$ follows the number of summing over the three expectations of Cobra-S128, i.e., $2^{12} + 2^8 + 2^4$, but the expected number of hits for a wrong subkey is much less than this value. Since the total number of control bits extracted in this attack is 21, the expected number of subkeys in the group is $2^{11}$. Hence we can retrieve the whole of master key pair with a data complexity of $2^{59}$ related-key chosen plaintexts and a time complexity of $2^{107}$ encryptions.

We now consider 18-round Cobra-F64b. In the first attack scenario, we use a 18-round related-key differential characteristic $(0, e_1) \rightarrow (e_1 \oplus t^{\ggg 8}, t)$ of Cobra-F64b with probability $2^{-56}$ (which includes the FT). This characteristic can be derived from Table 7 by cutting off the last two rounds, i.e., rounds 19 and 20. Thus if we use $2^{57}$ desired plaintext pairs (the filtering rate in Step 2 is $2^{-64} \cdot 2^6 = 2^{-58}$), we can extract at least 6 bits of the control vector $V$ by the same analysis as Cobra-S128. It follows that equation $V = C_L \oplus K_2 - (C_R \oplus K_3)^{\ggg 8}$

enables us to get 6 bits of key information, where $C_L$ is the left 32 bits of ciphertext and $C_R$ is the right 32 bits of ciphertext. Hence we can retrieve the whole of master key pair with a data complexity of $2^{58}$ related-key chosen plaintexts and a time complexity of $2^{128-6} = 2^{122}$ encryptions.

## 6 Conclusion

Three Cobra ciphers (Cobra-S128, Cobra-F64a, and Cobra-F64b) are considerably resistant against conventional attacks, e.g., the differential attack, the linear attack, and so on because they use data-dependent permutaions which are composed of the basic CP-boxes, $P_{2/1}$ (bit-controlled transpositons of two input bits). However, the very simple key schedule (i.e., the part of secret key is directly used in each round) and low diffusion of CP-boxes allow us to devise the related-key differential attacks on three Cobra ciphers.

In this paper, we presented the related-key attacks on Cobra-S128, Cobra-F64a and, Cobra-F64b. In the case of Cobra-S128, we can successfully recover 128-bit master keys of full-round Cobra-S128 with $2^{83}$ related-key chosen plaintexts and $2^{107}$ encryption units. In the cases of Cobra-F64a and Cobra-F64b, we can retrieve 128-bit master keys of 11-round Cobra-F64a and 18-round Cobra-F64b using $2^{59}$ and $2^{58}$ related-key chosen plaintexts, and $2^{107}$ and $2^{122}$ encryption units, respectively.

## 7 Acknowledgments

We would like to thank an anonymous reviewer for useful and interesting comments about this work.

## 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. M. Matsui, "Linear cryptanalysis method for DES cipher", *Advances in Cryptology - EUROCRYPTO'93*, LNCS 765, Springer-Verlag, 1993, pp. 386-397.
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. 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 The round function $Crypt^{(e)}$ used in Cobra-S128 and Cobra-F64

Fig. 6 represents the round function of Cobra-S128 and Fig. 7 represents the round function of Cobra-S64.

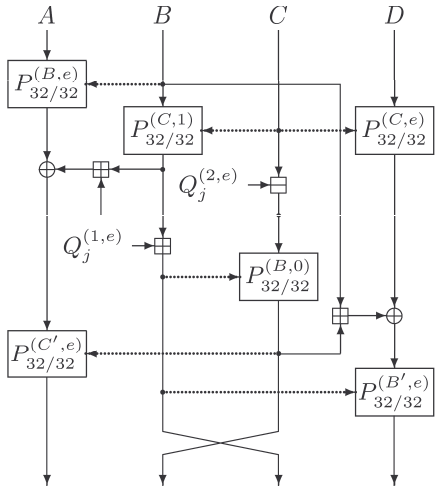


**Fig. 6.** Round function $Crypt^{(e)}$ of Cobra-S128

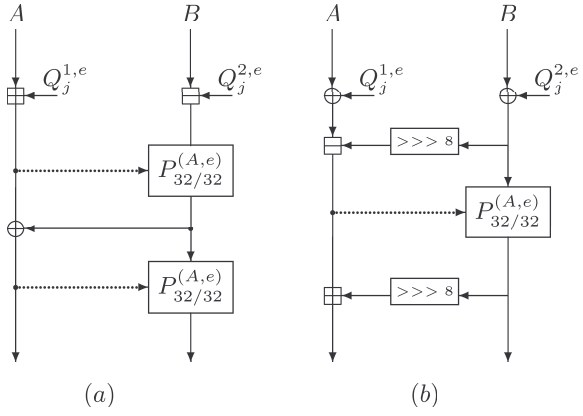


**Fig. 7.** (a) $Crypt^{(e)}$ of Cobra-F64a, (b) $Crypt^{(e)}$ of Cobra-F64b

# B Related-Key Differential Characteristics of Cobra-F64a and Cobra-F64b

Note that the probability $2^{-2}$ in the FT line of Table 6 is derived from the last $\boxplus$ operation. Also note that the probability $2^{-5}$ in the line of the $20th$ round of Table 7 is derived from $P1$ and the last $\boxplus$ operation.

**Table 6.** Related-Key Differential Characteristic of Cobra-F64a

| Round ($i$) | $\Delta RI^i$ | $\Delta RK^i$ | $P1/P2$ | Prob. |
|---|---|---|---|---|
| 1 | $(e_1, e_1)$ | $(0, e_1)$ | $2^{-3}/2^{-3}$ | $2^{-6}$ |
| 2 | $(0, e_1)$ | $(0, 0)$ | $2^{-6}/2^{-8}$ | $2^{-14}$ |
| 3 | $(e_1, e_1)$ | $(0, 0)$ | $2^{-8}/2^{-6}$ | $2^{-14}$ |
| 4 | $(e_1, 0)$ | $(e_1, 0)$ | $1/1$ | 1 |
| 5 | $(0, 0)$ | $(0, 0)$ | $1/1$ | 1 |
| 6 | $(0, 0)$ | $(0, 0)$ | $1/1$ | 1 |
| 7 | $(0, 0)$ | $(e_1, 0)$ | $2^{-3}/2^{-3}$ | $2^{-6}$ |
| 8 | $(0, e_1)$ | $(0, e_1)$ | $1/1$ | 1 |
| 9 | $(0, 0)$ | $(0, 0)$ | $1/1$ | 1 |
| 10 | $(0, 0)$ | $(0, 0)$ | $1/1$ | 1 |
| 11 | $(0, 0)$ | $(e_1, 0)$ | $2^{-3}/2^{-3}$ | $2^{-6}$ |
| 12 | $(0, e_1)$ | $(0, 0)$ | $2^{-6}/2^{-8}$ | $2^{-14}$ |
| FT | $(e_1, t)$ | $(0, 0)$ | $\cdot$ | $2^{-2}$ |
| Output | $(e_1, t)$ | $\cdot$ | $\cdot$ | $\cdot$ |
| Total | $\cdot$ | $\cdot$ | $\cdot$ | $2^{-62}$ |

**Table 7.** Related-Key Differential Characteristic of Cobra-F64b

| Round ($i$) | $\Delta RI^i$ | $\Delta RK^i$ | $P1$ | Prob. |
|---|---|---|---|---|
| 1 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 2 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 3 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 4 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 5 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ |
| $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ |
| $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ |
| 17 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 18 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 19 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-3}$ |
| 20 | $(0, e_1)$ | $(e_1, e_1)$ | $2^{-3}$ | $2^{-5}$ |
| FT | $(e_1 \oplus t^{\ggg 8}, t)$ | $(e_1, e_1)$ | $\cdot$ | $\cdot$ |
| Output | $(e_1 \oplus t^{\ggg 8}, t)$ | $\cdot$ | $\cdot$ | $\cdot$ |
| Total | $\cdot$ | $\cdot$ | $\cdot$ | $2^{-62}$ |