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 of

* 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

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 244–262, 2005.

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

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., $e_1 = (1, 0, \cdots, 0)$.