International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.355-360
http://dx.doi.org/10.14257/ijsia.2016.10.1.32

Distinguishing Attack on CPB-Based Cipher COSB-128

[1] Tran Song Dat Phuc, [1,*] Changhoon Lee

[1]*Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung-ro, Nowon-gu, Seoul, 139-743, South Korea, datphuc_89@yahoo.com, chlee@seoultech.ac.kr*

Abstract

COSB-128 is a type of fast controllable permutation block (CPB), which is designed to ensure a high speed of data transformation and high stability to differential analysis. In this paper, we present the possibility to distinguish between a 10-round COSB-128 and a 128-bit random permutation through a full 10-round related-key difference characteristic by proposing a distinguishing attack with high probability on this cipher. This attack is another result from previous study of related-key attack on COSB-128 [2]. From that point, it reveals the potential to extend to the related-key recovery attack on this algorithm in the future.

Keywords*: Controllable permutation block (CPB), Controllable operational substitution block (COSB), Distinguishing Attack, Cryptanalysis*

1. Introduction

Recently, the use of network-based devices and services has increased gradually. Thence, security becomes an essential interest, which is acquired not only to be strong with most unknown attacks, but also to be optimized on hardware implementations or specialized applications. With these criteria, designing cipher is a cryptographic primitive approach in modern applied cryptography.

It has some designs of cipher showed their advantage, such as CIKS-1 [3], CIKS-128 [4], Cobra-H64 [5], Cobra-H128 [5]… based on DDP concept; or SCO-1, SCO-2, SCO-3 [6]… based on COS; Eagle-64 [8], Eagle-128 [7]… based on DDO concept - to enhance the DDP-based ciphers. Although there are many well-known ciphers, with different specifications and characteristics, the security of them is under consideration.

COSB-128 [1] is a 128-bit block cipher with a 256-bit key, the number of round is 10. It uses the concept of fast controllable permutation blocks (CPB) and controlled operational substitution (COS). This cipher is expected to be high performance in hardware-software implementations as well as high stability with differential analysis.

This paper shows that this type of ciphers is still vulnerable to related-key differential attack, and the possibility to distinguish between a 10-round COSB-128 with 128-bit random permutation through 10-round related-key difference characteristics. We propose a distinguishing attack with high probability 2^{-48}, requiring data complexity of 2^{50} related-key chosen plaintexts. This result is another study with another characteristic of related-key attack on COSB-128 [2].

2. Description of COSB-128

First, we introduce the notations which are used in the paper.

- $e_{i,j}$: 32-bit binary string in which the i^{th} bit and j^{th} bit are one and the others are zeroes (*e.g.*, $e_{1,3}$ = (1, 0, 1, 0,…,0)).
- ΔI_r : input difference in round r.
- ΔK_r : round key difference in round r.

ISSN: 1738-9976 IJSIA

The values of control ciphers V_1, $V_2 \in GF(2)^{192}$ is presented through the diagram of transformation of the control vector H, with the ciphers V_i, with i = 1,2.

$$V_i = \{W_1^{(i)} | W_2^{(i)} | W_3^{(i)} | W_4^{(i)} | W_5^{(i)} | W_6^{(i)}\}.$$

The output values of $W_j^{(i)} \in GF(2)^{32}$ are defined:

$$W_1^{(1)} = A_l,\ W_2^{(1)} = A_h^{<<<1},\ W_3^{(1)} = (A \oplus K_1)_h^{<<<18},$$

$$W_4^{(1)} = (A \oplus K_1)_l^{<<<4},\ W_5^{(1)} = (A \oplus K_2)_l^{<<<8},\ W_6^{(1)} = (A \oplus K_2)_h^{<<<16},$$

$$W_1^{(2)} = A_l,\ W_2^{(2)} = A_h^{<<<1},\ W_3^{(2)} = (A \oplus K_4)_h^{<<<18},$$

$$W_4^{(2)} = (A \oplus K_4)_l^{<<<4},\ W_5^{(2)} = (A \oplus K_3)_l^{<<<8},\ W_6^{(1)} = (A \oplus K_3)_h^{<<<16},$$

where indices l and h denote 32 lower-order or higher-order digits of the vector transformed.

The substitution transformation **G** uses $\Psi(A, Q)$, where A, $Q \in GF(2)^{64}$, $Q = K_1 \oplus K_3$ for odd cycles and $Q = K_2 \oplus K_4$ for even cycles.

$$\Psi(A, Q) = (A_1 \times A_3 \times Q_2 \times A_5 \times A_6 \times A_8) \oplus (A_1 \times A_3 \times A_6 \times A_8) \oplus (A_1 \times Q_2 \times A_5 \times A_8) \oplus (A_3 \times Q_2 \times A_5 \times A_6) \oplus (A_1 \times Q_2 \times A_6) \oplus (A_3 \times A_5 \times A_8) \oplus (A_1 \times A_3 \times Q_2) \oplus (A_5 \times A_6 \times A_8) \oplus (A_1 \times A_4) \oplus (Q_1 \times A_6) \oplus (A_2 \times A_8) \oplus (A_3 \times Q_3) \oplus (Q_2 \times A_7) \oplus (A_5 \times Q_4) \oplus A_0 \oplus Q_0,$$

In which:

$$A_0 = (a_1, a_1, \ldots, a_n),\ A_1 = (a_n, a_1, \ldots, a_{n-1}), \ldots,$$
$$A_j = (a_{n-j+1}, \ldots, a_n, a_1, \ldots, a_{n-j}),\ Q_0 = (q_1, q_1, \ldots, q_n),$$
$$Q_1 = (q_n, a_1, \ldots, q_{n-1}), \ldots,\ Q_j = (q_{n-j+1}, \ldots, q_n, q_1, \ldots, q_{n-j}).$$

The master key Z = (z_1, z_2, z_3, z_4) produces the round keys is given in following table.

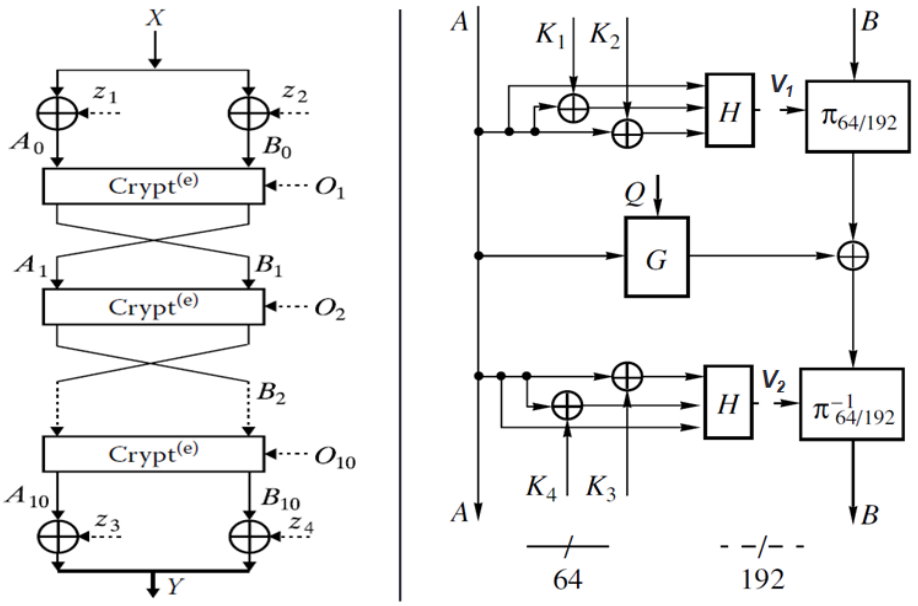

Figure 1. Structure of Crypt of COSB-128

Table1. Schedule of Round Keys

Key	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_9	O_{10}
K_1	z_1	z_4	z_3	z_2	z_4	z_3	z_1	z_2	z_3	z_1
K_2	z_2	z_1	z_4	z_3	z_2	z_4	z_3	z_1	z_2	z_3
K_3	z_3	z_2	z_1	z_4	z_1	z_2	z_4	z_3	z_4	z_2
K_4	z_4	z_3	z_2	z_1	z_3	z_1	z_2	z_4	z_1	z_4

3. Distinguishing Attack on COSB-128

We describe some properties of (Crypt) function of COSB-128 allow to construct related-key difference characteristics.

a. / Let $\Pr(\boldsymbol{F}_{2/1})(\Delta Y/ \Delta X, \Delta V)$ be a probability to have the output difference ΔY of $\boldsymbol{F}_{2/1}$, where ΔX is input difference and ΔV is controlling vector difference.

$\Pr(\boldsymbol{F}_{2/1})((0, 0)/ (0, 0), 0) = 1$

$\Pr(\boldsymbol{F}_{2/1})((0, 1)/ (0, 1), 0) = 2^{-1}$, $\Pr(\boldsymbol{F}_{2/1})((1, 0)/ (0, 1), 0) = 2^{-1}$

$\Pr(\boldsymbol{F}_{2/1})((0, 1)/ (1, 0), 0) = 2^{-1}$

$\Pr(\boldsymbol{F}_{2/1})(\Delta Y/ \Delta X, 1) = 2^{-2}$, for any ΔY and ΔX

b. / Let $\Pr(\boldsymbol{F}^{(e)}_{64/192})(\Delta Y/ \Delta X, \Delta V)$ be a probability to have the output difference ΔY of $\boldsymbol{F}^{(0)}_{64/192}$, $\boldsymbol{F}^{(1)}_{64/192}$, where ΔX and ΔV are input and controlling vector difference.

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(0/ 0, 0) = \Pr(\boldsymbol{F}^{(1)}_{64/192})(0/ 0, 0) = 1$

$\Pr(\boldsymbol{F}^{(0)}_{64/192\ (V)}(X) \oplus \boldsymbol{F}^{(0)}_{64/192\ (V \oplus ei)}(X) = e_i) = 2^{-2}$

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_1, K_2) \oplus H(A, K_1 \oplus e_{64}, K_2) = e_{124}) = 1$ $\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_1, K_2) \oplus H(A, K_1, K_2 \oplus e_{64}) = e_{152}) = 1$

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_1, K_2) \oplus H(A, K_1 \oplus e_{64}, K_2 \oplus e_{64}) = e_{124,\ 152}) = 1$

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_3, K_4) \oplus H(A, K_3 \oplus e_{64}, K_4) = e_{124}) = 1$

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_3, K_4) \oplus H(A, K_3, K_4 \oplus e_{64}) = e_{152}) = 1$

$\Pr(\boldsymbol{F}^{(0)}_{64/192})(H(A, K_3, K_4) \oplus H(A, K_3 \oplus e_{64}, K_4 \oplus e_{64}) = e_{124,\ 152}) = 1$

c. / Probability of transformation **G**:

$\Pr(G_Q(A) \oplus G_{Q \oplus e_{64}}(A) = 0) = 2^{-1}$ (when $q_{64} = 1$)

$\Pr(G_Q(A) \oplus G_{Q \oplus e_{64}}(A) = e_{64}) = 2^{-1}$ (when $q_{64} = 0$).

We assign to encrypt the plaintext pairs (P, P*) under the key pairs (K, K*), in which $\alpha = P \oplus P^* = (e_{64}, e_{64})$, and $\Delta K = K \oplus K^* = (e_{64}, e_{64}, 0, 0)$; to get the corresponding ciphertext pairs (C, C*).

So, as the **Table 2.**, we can construct a 10-round related-key differential characteristic $\alpha \rightarrow \beta$, in which $\beta = (0, 0)$ for round 1~10 of COSB-128 with probability 2^{-48}.

Table2. Related-Key Difference Characteristics of 10-Round of COSB-128

Round(r)	ΔI_r	(ΔK_r)	Probability
IT	$\alpha = (e_{64}, e_{64})$	(e_{64}, e_{64})	1
1	(0, 0)	$(e_{64}, e_{64}, 0, 0)$	2^{-5}
2	(0, 0)	$(0, e_{64}, e_{64}, 0)$	2^{-5}
3	(0, 0)	$(0, 0, e_{64}, e_{64})$	2^{-5}
4	(0, 0)	$(e_{64}, 0, 0, e_{64})$	2^{-5}
5	(0, 0)	$(0, e_{64}, e_{64}, 0)$	2^{-5}
6	(0, 0)	$(0, 0, e_{64}, e_{64})$	2^{-5}
7	(0, 0)	$(e_{64}, 0, 0, e_{64})$	2^{-5}
8	(0, 0)	$(e_{64}, e_{64}, 0, 0)$	2^{-5}
9	(0, 0)	$(0, e_{64}, 0, e_{64})$	2^{-4}
10	(0, 0)	$(e_{64}, 0, e_{64}, 0)$	2^{-4}
FT	(0, 0)		1
Output	$(0, 0) = \beta$		
Total			2^{-48}

The procedure of distinguishing attack of COSB-128 is as follows.

1. Choose a pool of 2^{49} plaintext pairs (P_i, P^*_i) with difference $\alpha = P \oplus P^* = (e_{64}, e_{64})$. Then, with the chosen plaintext attack, we encrypt the plaintext pairs using (K, K^*) to get the ciphertext pairs (C, C*), in which $\Delta K = K \oplus K^* = (e_{64}, e_{64}, 0, 0)$.
2. For each ciphertext pair (C, C*), check if $C \oplus C^* = (0, 0)$.
3. If the number of pairs passing Step 2 is greater than or equal to 2, the given cipher texts were generated through a 10-round COSB-128. Otherwise, the given ciphertexts were generated using 128-bit random permutation.

This attack requires a pool of 2^{49} plaintext pairs and data complexity is 2^{50} related-key chosen plaintexts. If the given ciphertexts were generated by using a full 10-round COSB-128, this attack can distinguish between a full 10-round COSB-128 and a 128-bit random permutation with probability 1. Otherwise, the probability that the attack outputs in which the given ciphertexts were generated by using a full 10-round COSB-128 is low.

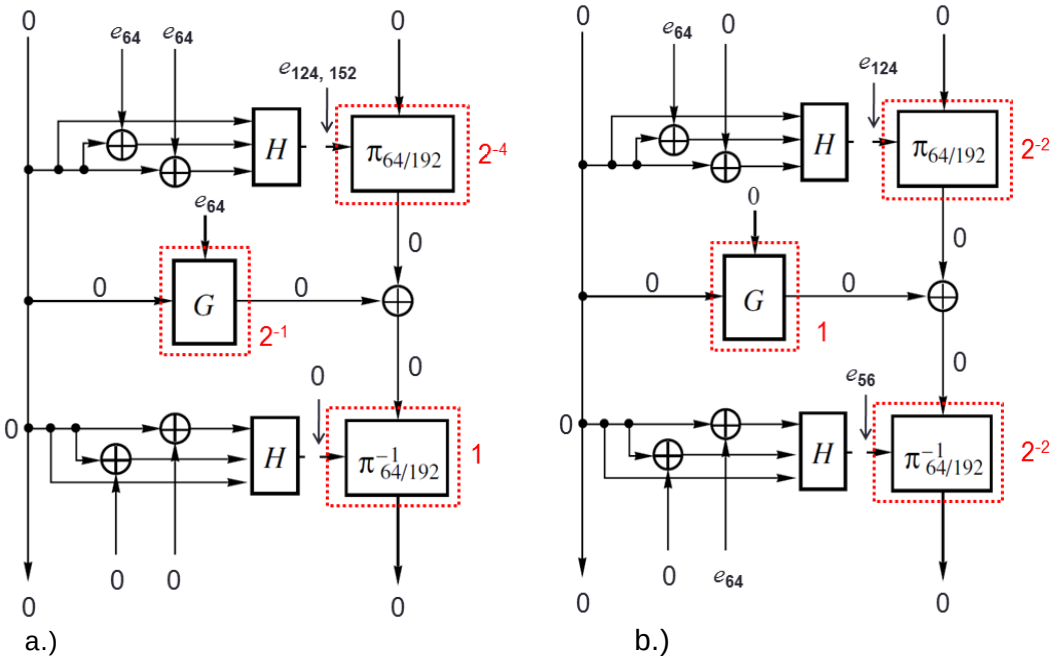

Figure 2. Propagation of Difference in a.) 1st Round and b.) 10th Round of COSB-128

4. Conclusion

In this paper, we presented the possibility to distinguish between a 10-round COSB-128 with 128-bit random permutation through 10-round related-key difference characteristics, by proposing a distinguishing attack with high probability on a full round this cipher. This attack requires a pool of 2^{49} plaintext pairs and data complexity of 2^{50} related-key chosen plaintexts. The method is expected to extend a related-key recovery attack on this type of ciphers in later research.

References

[1] N. Moldovyan, A. Moldovyan , M. Eremeev , "Protective Data Transformations in ACSs on the Basic of a New Primitive," Automation and Remote Control, vol. 63, no. 12, **(2002)**, pp. 1996-2013.
[2] T. Phuc, C. Lee, "Related-Key Differential Attacks on COSB-128", International Journal of Distributed Sensor Networks, vol. 2015 (**2015**), Article ID 617972, 8 pages.
[3] A. Moldovyan, N. Moldovyan, "A cipher Based on Data-Dependent Permutations," Journal of Cryptology, vol. 15, no. 1, **(2002)**, pp. 61-72.
[4] N. Goots, B. Izotov, A. Moldovyan, N. Moldovyan, "Modern cryptography: Protect Your Data with Fast Block Ciphers", Wayne, **(2003)**, A-LIST Publish.
[5] N. Sklavos, N. Moldovyan, O. Koufopavlou, "High Speed Networking Security: Design and Implementation of Two New DDP-Based Ciphers", In: Mobile Networks and Applications-MONET, **(2005)**, vol. 25, no. 1-2, pp. 219-231.
[6] N. Moldovyan , "On Cipher Design Based on Switchable Controlled Operations", In: MMM-ACNS 2003, LNCS, **(2003)**, vol. 2776, pp. 316-327, Springer, Heidelberg.
[7] N. Moldovyan, A. Moldovyan, M. Eremeev, N. Sklavos , "New Class of Cryptographic Primitives and Cipher Design for Networks Security," International Journal of Network Security, vol. 2, no. 2, **(2006)**, pp. 114-225.
[8] N. Moldovyan , A. Moldovyan , M. Eremeev, D. Summerville , "Wireless Networks Security and Cipher Design Based on Data-Dependent Operations: Classification of the FPGA Suitable Controlled Elements", In: Proceedings of CCCT04, **(2004)**, vol. VII, pp. 123-128, Texas, USA.
[9] Y. Ko, C. Lee, S. Hong, J. Sung, S. Lee, "Related-key Attacks on DDP Based Ciphers: CIKS-128 and CIKS-128H," Indocrypt'04, LNCS 3348, Springer-Verlag, **(2004)**, pp. 191-205.
[10] C. Lee, J. Kim, J. Sung, S. Hong, S. Lee, "Related-key differential attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b" MYCRYTP'05, LNCS 3715, Springer-Verlag, **(2005)**, pp. 245-263.

[11] K. Jeong, C. Lee, J. Kim, S. Hong, "Security analysis of the SCO-family using key schedules," Information Sciences 179, **(2009)**, pp. 4232-4242.

Authors

Tran Song Dat Phuc, He received his Bachelor Degree in Information Technology from HCMC University of Technology, Vietnam in 2011; and Master's Degree in Computer Science and Engineering from Seoul National University of Science and Technology in Korea in 2015. He is currently a PhD candidate at Information Security Lab at Seoul National University of Science and Technology in Korea. His main research interests are Information Security, Network Security, and Digital Forensics.

Dr. Changhoon Lee, He received his Ph.D. in the Graduate School of Information Management and Security (GSIMS) from Korea University in Korea. In 2008, he was a research professor at the Center for Information Security Technologies in Korea University. In 2009-2011, he was a professor in the School of Computer Engineering in Hanshin University. He is now a professor at the Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech) in Korea. He has been serving not only as chairs, program committee, or organizing committee chair for many international conferences and workshops but also as an (guest) editor for international journals by some publishers. His research interests include information security, cryptography, digital forensics, smart grid security, computer theory *etc*. He is currently a member of the IEEE, IEEE Computer Society, IEEE Communications, IACR, KIISC, KDFS, KIPS, KITCS, KMMS, KONI, and KIIT societies.

