情報保護學會論文誌
第18卷 第4號, 2008. 8

블록 암호 SCO-1에 대한 안전성 분석*

정 기 태†, 이 창 훈, 김 종 성, 홍 석 희‡
고려대학교 정보보호기술연구센터

Security Analysis on the Full-Round SCO-1*

Kitae Jeong†, Changhoon Lee, Jongsung Kim, Seokhie Hong‡
Center for Information Security Technologies, Korea University

요 약

본 논문에서는 블록 암호 SCO-1[12]에 대한 연관키 차분 공격을 소개한다. 본 논문에서 소개하는 공격은 SCO-1에 대한 첫 번째 공격이며 2^{61}개의 연관키 선택 암호문을 이용하여 $2^{120.59}$의 SCO-1 복호화 연산을 수행하여 SCO-1의 128-비트 비밀키를 복구한다.

ABSTRACT

In this paper we show that the full-round SCO-1[12] is vulnerable to the related-key differential attack. The attack on the full-round SCO-1 requires 2^{61} related-key chosen ciphertexts and $2^{120.59}$ full-round SCO-1 decryptions. This work is the first known attack on SCO-1.

Keywords : Block Cipher, SCO-1, Data-Dependent Operation, Related-Key Differential Attack, Cryptanalysis

Ⅰ. Introduction

Recently, several DDP (Data Dependent Permutation) -based ciphers have been proposed for hardware implementations with low cost, e.g., SPECTR-H64[3], CIKS-family (CIKS-1[13] and CIKS-128[1]), and the Cobra-family (Cobra-S128[2], Cobra-F64a[2], Cobra-F64b[2], Cobra-H64[16] and Cobra-H128[16]). Since all of them use a very simple key schedule in order to 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, most of them have been cryptanalyzed due to a linearity of DDP and simply designed key scheduling algorithms[5-11]. As a counter proposal for eliminating a linearity of DDP and improving the security of DDP-based ciphers, the new DDP-like DDO (Data Dependent Operation) that arbitrarily change the weight of the transformed binary vectors, called COS (Controlled Operational Substitution), has been developed and the COS-based cipher SCO-1[12] has been proposed. It is a 64-bit block cipher with a 128-bit key and the number of 8 rounds, which can overcome the problem of the weak keys and homogeneity of the encryption transformation while the simple key schedule is used.

접수일 : 2007년 12월 21일; 채택일 : 2008년 4월 19일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))
† 주저자, kite@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr

[Table 1] Result of our attack on SCO-1

Number of Attacked Rounds (Total Rounds)	Data Complexity	Time Complexity
8 (8)	2^{61} RK-CC	$2^{120.59}$

RK-CC: Related-Key Chosen Ciphertexts
Time: Decryption units

In this paper, however, we show that the related-key differential attack can be applied to devise a key recovery attack on the full-round SCO-1. This attack requires 2^{61} related-key chosen ciphertexts and $2^{120.59}$ full-round SCO-1 decryptions. This work is the first known cryptanalytic result on SCO-1. [Table 1] summarizes our attack with its complexities.

This paper is organized as follows; In Section 2, we briefly describe SCO-1 and its structural properties. In Section 3, we present a related-key differential attack on SCO-1. Finally, we conclude in Section 4.

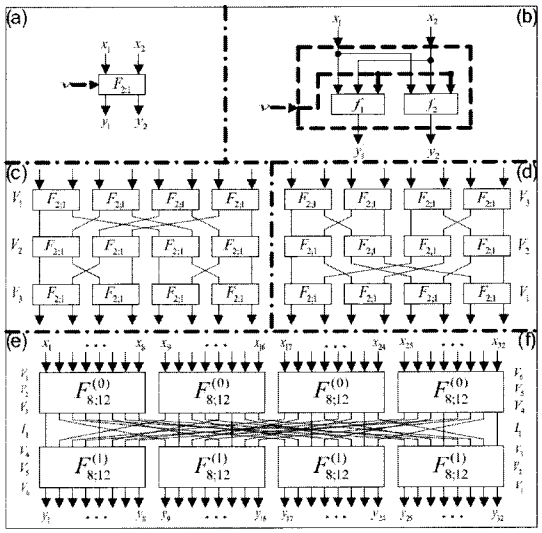
Ⅱ. Description of SCO-1

In this section, we introduce SCO-1 and its structural properties. The following notations are used throughout the paper. A bit index 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., $e_{1,3}=(1,0,1,\cdots,0)$.
- $\oplus$: Bitwise-XOR operation.
- $\boxplus$: addition modulo 2^{32}.
- $\boxminus$: subtraction modulo 2^{32}.
- $\ggg$: right cyclic rotation.

2.1 COS-Boxes

In this subsection, we introduce COS-boxes which are one of the major components of SCO-1. For $e\in\{0,1\}$, a COS-box $F_{n;m}^{(e)}(X,V)$ taking a n-bit input vector X outputs a n-bit value Y controlled by a m



[Fig. 1] (a) $F_{2;1}$, (b) $F_{2;1}$, (c) $F_{8;12}^{(0)}$, (d) $F_{8;12}^{(1)}$, (e) $F_{32;96}^{(0)}$, (f) $F_{32;96}^{(1)}$

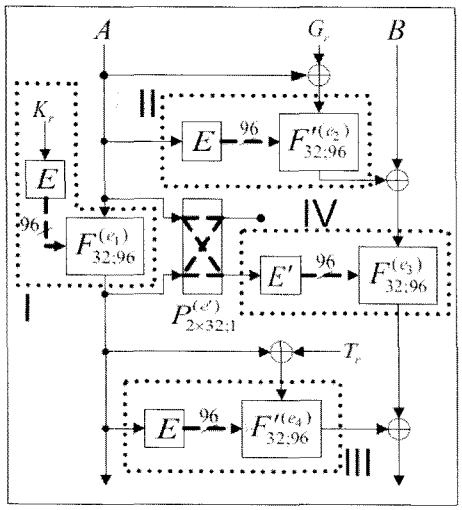
-bit controlling vector V. As shown in [Fig. 1], it is constructed by combining the elementary building block $F_{2;1}$ which is defined as $F_{2;1}(x_1,x_2,v)=(x_1(v\oplus1)\oplus x_2 v, x_1\oplus x_2(v\oplus1))$. That is, $(y_1,y_2)=(x_1,x_1\oplus x_2)$ for $v=0$ and $(y_1,y_2)=(x_2,x_1)$ for $v=1$.

$F_{8;12}^{(e)}$ containing three active layers is used as a main building block which induces the six-layer box $F_{32;96}^{(e)}$. Because of their symmetric structure, the mutual inverses of $F_{n;m}^{(0)}$ and $F_{n;m}^{(1)}$ differ only in the distribution of controlling bits over $F_{2;1}$, e.g., $F_{32;96}^{(0)}(\cdot,V)$and $F_{32;96}^{(1)}(\cdot,V')$ are mutual inverses when $V=(V_1,V_2,V_3)$ and $V'=(V_3,V_2,V_1)$. Note that the permutational involution I_1 is performed as follows;

$$I_1=(1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32).$$

2.2 Description of SCO-1

SCO-1 is a 64-bit block cipher with a 128-bit key $Q=(Q_1,Q_2,Q_3,Q_4)$ and the number of 8 rounds. It is composed of the round function $Crypt^{(e)}$, the initial transformation (IT) and the final transformation (FT), where $e=0$ and $e=1$ denotes encryption and



(Fig. 2) The round encryption function $Crypt^{(0)}$ of SCO-1

decryption modes, respectively. The following is the 8-round encryption procedure of SCO-1 $(e=0)$. In the decryption mode, P, $K_r^{(0)}$, $G_r^{(0)}$ and $T_r^{(0)}$ are just replaced with C, $K_r^{(1)}$, $G_r^{(1)}$ and $T_r^{(1)}$, respectively.

1. A 64-bit input block P is divided into two subblocks P_L and P_R.
2. $(A,B)\leftarrow(P_L,P_R)$.
3. Perform the initial transformation : $A=A\oplus G^{(0)}$ and $B=B\oplus T^{(0)}$.
4. For $r=1$ to 7 do :
   - $(A,B)\leftarrow Crypt^{(0)}\left(A,B,K_r^{(0)},G_r^{(0)},T_r^{(0)}\right)$, where $K_r^{(0)},G_r^{(0)}$ and $T_r^{(0)}$ are the r-th round keys;
   - Swap data subblocks : $(A,B)\leftarrow(B,A)$;
5. $(A,B)\leftarrow Crypt^{(0)}\left(A,B,K_8^{(0)},G_8^{(0)},T_8^{(0)}\right)$;
6. Perform the final transformation : $(A,B)\leftarrow\left(A\oplus G_{FT}^{(0)},B\oplus T_{FT}^{(0)}\right)$;
7. $(C_L,C_R)\leftarrow(A,B)$;
8. Return the ciphertext block $C=(C_L,C_R)$.

The COS-boxes $F^{(e_i)}_{32;96}$ $(i=1,2,3,4)$ are constructed by using the $F_{2;1}$ as depicted in [Fig. 1]. We denote that $F'^{(0)}_{32;96}=F^{(1)}_{32;96}$ and $F'^{(1)}_{32;96}=F^{(0)}_{32;96}$. For the controlling value e', $P^{(e')}_{2\times32;1}(x_1,x_2)$ taking two 32-bit input values x_1 and x_2 outputs two 32-bit values y_1 and y_2 as $P^{(e')}_{2\times32;1}(x_1,x_2)=\left(e'(x_1\oplus x_2)\oplus x_1,e'(x_1\oplus x_2)\oplus x_2\right)$. That is $(y_1,y_2)=(x_1,x_2)$ for $e'=0$ and $(y_1,y_2)=(x_2,x_1)$ for $e'=1$.

The extension box E used to form the controlling vector is described by [Table 2], where $W=(w_1,w_2,\cdots,w_{32})$ and $V=(V_1,V_2,\cdots,V_6)$ are input and output vectors of E, respectively. The second-type extension box E' is defined as $E'(W)=E(W^{\lll 16})$.

SCO-1 uses a simple keyschedule. A 128-bit secret key Q is divided into four 32-bit blocks, i.e., $Q=(Q_1,Q_2,Q_3,Q_4)$ and then subkeys $Q_i\,(1\le i\le 4)$ are directly used in $Crypt^{(e)}$. [Table 3] presents the specification of switching bits (e_1,e_2,e_3,e_4,e') and round subkeys of SCO-1.

2.3 Properties of SCO-1

In this subsection, we describe some properties for $F^{(e)}_{32;96}$ which allow to construct a related-key differential characteristic of SCO-1.

Property 1. Let $\Pr_{(F_{2;1})}(\Delta Y/\Delta X,\Delta V)$ be a probability to have the output difference ΔY of $F_{2;1}$, when the input difference is ΔX and the difference at the controlling input is ΔV. Then we have the followings;

(1) $\Pr_{(F_{2;1})}((0,0)/(0,0),0)=1$.

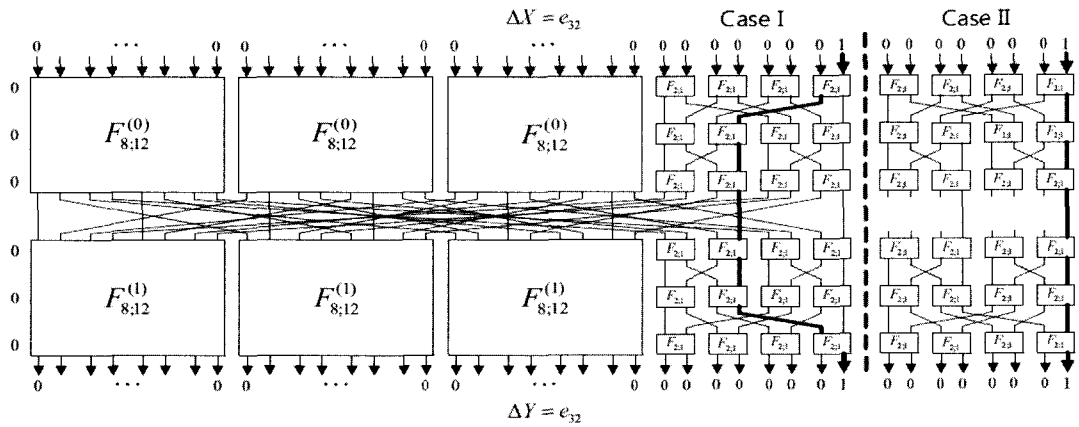
(2) $\Pr_{(F_{2;1})}((0,1)/(0,1),0)=\Pr_{(F_{2;1})}((1,0)/(0,1),0)=2^{-1}$.

(Table 2) The extension box E

V_1	w_7	w_8	w_1	w_2	w_{16}	w_{15}	w_{10}	w_9	w_5	w_6	w_3	w_4	w_{11}	w_{12}	w_{13}	w_{14}
V_2	w_9	w_{10}	w_{11}	w_{12}	w_1	w_2	w_7	w_8	w_{13}	w_{14}	w_{15}	w_{16}	w_5	w_6	w_3	w_2
V_3	w_{13}	w_{14}	w_{15}	w_{16}	w_5	w_6	w_3	w_4	w_1	w_2	w_7	w_8	w_9	w_{10}	w_{11}	w_{12}
V_4	w_{21}	w_{22}	w_{29}	w_{30}	w_{25}	w_{26}	w_{23}	w_{24}	w_{31}	w_{32}	w_{27}	w_{28}	w_{17}	w_{18}	w_{19}	w_{20}
V_5	w_{31}	w_{32}	w_{27}	w_{28}	w_{17}	w_{18}	w_{19}	w_{20}	w_{29}	w_{30}	w_{25}	w_{26}	w_{21}	w_{22}	w_{23}	w_{24}
V_6	w_{19}	w_{20}	w_{23}	w_{24}	w_{27}	w_{28}	w_{29}	w_{30}	w_{21}	w_{22}	w_{17}	w_{18}	w_{32}	w_{31}	w_{25}	w_{26}

[Table 3] The specification of switching bits and round subkeys of SCO-1

Round	e=0/1			e=0					e=1				
r	$K_r^{(e)}$	$G_r^{(e)}$	$T_r^{(e)}$	e_1	e_2	e_3	e_4	e'	e_1	e_2	e_3	e_4	e'
IT	·	Q_2	Q_1	·	·	·	·	·	·	·	·	·	·
1	Q_1	Q_2	Q_3	1	0	1	0	0	0	0	1	1	0
2	Q_4	Q_1	Q_2	0	1	1	1	1	1	1	1	1	0
3	Q_3	Q_4	Q_1	0	0	0	0	0	0	0	1	0	1
4	Q_2	Q_3	Q_4	1	0	1	1	0	0	0	0	1	0
5	Q_2	Q_4	Q_3	1	1	1	0	1	0	1	0	0	1
6	Q_3	Q_1	Q_4	1	0	0	0	0	1	0	1	0	1
7	Q_4	Q_2	Q_1	0	1	0	1	1	1	1	0	1	0
8	Q_1	Q_3	Q_2	1	1	0	0	1	0	0	0	0	1
FT	·	Q_2	Q_1	·	·	·	·	·	·	·	·	·	·



[Fig. 3]. $\Pr_{(F_{32;96}^{(0)})}(e_{32}/e_{32},0)=2^{-5}$

(3) $\Pr_{(F_{21})}((0,1)/(1,0),0)=\Pr_{(F_{21})}((1,1)/(1,0),0)=2^{-1}$.

(4) $\Pr_{(F_{21})}((1,0)/(1,1),0)=\Pr_{(F_{21})}((1,1)/(1,1),0)=2^{-1}$

(5) $\Pr_{(F_{21})}(\Delta Y/\Delta X,1)=2^{-2}$ for any ΔX and ΔY.

The above properties are also extended into the following properties.

Property 2. $\Pr_{(COS)}(\Delta Y/\Delta X,\Delta V)$ be a probability to have the output difference ΔY, when $COS \in \{F_{32;96}^{(0)}, F_{32;96}^{(1)}\}$, the input difference is ΔX and the difference at the controlling input is ΔV. Then we have the followings;

(1) $\Pr_{(F_{32;96}^{(0)})}(0/0,0)=\Pr_{(F_{32;96}^{(1)})}(0/0,0)=1$.

(2) $\Pr_{(F_{32;96}^{(0)})}(e_{32}/e_{32},0)=\Pr_{(F_{32;96}^{(1)})}(e_{32}/e_{32},0)=2^{-5}$.

(3) $\Pr_{(F_{32;96}^{(0)})}(0/0,E(e_{32}))=\Pr_{(F_{32;96}^{(1)})}(0/0,E(e_{32}))=2^{-6}$, where $E(e_{32})=(0,0,0,e_{10},e_2,e_{13})$.

(4) $\Pr_{(F_{32;96}^{(0)})}(0/0,E'(e_{32}))=\Pr_{(F_{32;96}^{(1)})}(0/0,E'(e_{32}))=2^{-6}$, where $E'(e_{32})=(e_5,e_{12},e_4,0,0,0)$.

(5) $\Pr_{(F_{32;96}^{(0)})}(0/e_{32},E(e_{32}))=2^{-8}$.

Here, we focus on the proof of Property 2-(2) $\Pr_{(F_{32;96}^{(0)})}(e_{32}/e_{32},0)=2^{-5}$. As shown in [Fig. 3], there are two cases that the output difference ΔY of $F_{32;96}^{(0)}$ is e_{32} with the input difference $\Delta X=e_{32}$ and the controlling input difference $\Delta V=0$. In [Fig. 3], bold lines mean an active difference. Using Property 1, active differences through a $F_{2;1}$ hold with probability

2^{-1}. It implies that each case holds with probability 2^{-6}. So the probability that the output difference ΔY of $F^{(0)}_{32;96}$ is e_{32} with the input difference $\Delta X = e_{32}$ and the controlling input difference $\Delta V = 0$ is 2^{-5}. Other properties are proved similarly to Property 2-(2).

Ⅲ. Related-Key Differential Attack on SCO-1

Now, we describe a related-key differential attack on the full-round SCO-1. As stated before, the key schedule of SCO-1 is very simple, i.e., round keys are only 32-bit parts of a 128-bit secret key, and there are many useful properties of $F^{(0)}_{32;96}$ and $F^{(1)}_{32;96}$ which allow to construct a good related-key differential characteristic.

We consider the situation that we decrypt ciphertexts $C=(C_L, C_R)$ and $C^*=(C^*_L, C^*_R)$ under keys K and K^* such that $\alpha = C \oplus C^* = (0,0)$, $\Delta K = K \oplus K^* = (0, e_{32}, 0, 0)$, respectively. Then, as shown in [Table 4], we construct a full-round related-key differential characteristic $\alpha \rightarrow \beta$ with probability 2^{-57}, where $\beta = (A \oplus e_{32}, ?)$. Here, "?" denotes a 32-bit unknown difference and the set $A = \{\Delta Y \mid F^{(0)}_{32;96}(e_{32}, 0) = \Delta Y\}$ is the set of all possible output differences of $F^{(0)}_{32;96}(e_{32}, 0)$. Round r in [Table 4] means round $9-r$ in encryption process of SCO-1 $(r = 1, \cdots, 8)$ and Part I, II, III and IV are indicated in [Fig. 2].

As shown in [Fig. 4], the set of all input difference of $F_{2;1}$ except the last row is $\{(0,0),(0,1)\}$ by Property 1. Thus the set of all possible input differences of $F_{2;1}$ in the last row is $\{(0,0),(0,1),(1,0)\}$. So the set of all possible output difference of $F_{2;1}$ in the last row is $\{(0,0),(0,1),(1,0),(1,1)\}$. Hence A consists of 48 binary strings of which weights are 1 or 2. That is, $A = \{e_i \mid i \in \{1,2,\cdots,31,32\}\} \cup \{e_{i,j} \mid (i,j) \in \{(1,2),(3,4),\cdots, (31,32)\}\}$.

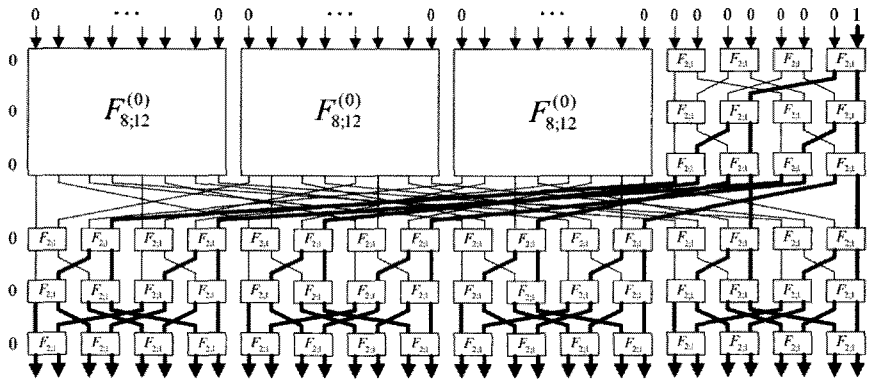
[Fig. 5-(a)] shows the first round characteristic after the IT step. In Part I, the probability that $F^{(0)}_{32;96}(e_{32}, E(0)) = e_{32}$ is 2^{-5} by Property 2-(2). In Part II and Part IV, the probability that $F'^{(0)}_{32;96}(0, E(e_{32})) = F^{(1)}_{32;96}(0, E'(e_{32})) = 0$ is 2^{-6} by Property 2-(3) and (4), respectively. Finally, the probability that $F'^{(1)}_{32;96}(e_{32}, E(e_{32})) = 0$ is 2^{-8} by Property 2-(5) in Part III. Thus, the output difference of the first round including the swapping operation is $(0, e_{32})$ with probability 2^{-25}, when the input difference is $(e_{32}, 0)$. The other round characteristics are explained similarly to the first round.

We are now ready to show how to exploit the above characteristic with probability 2^{-57} to attack the full-round SCO-1. We assume that SCO-1 cipher uses the secret key K and its related key K^* with

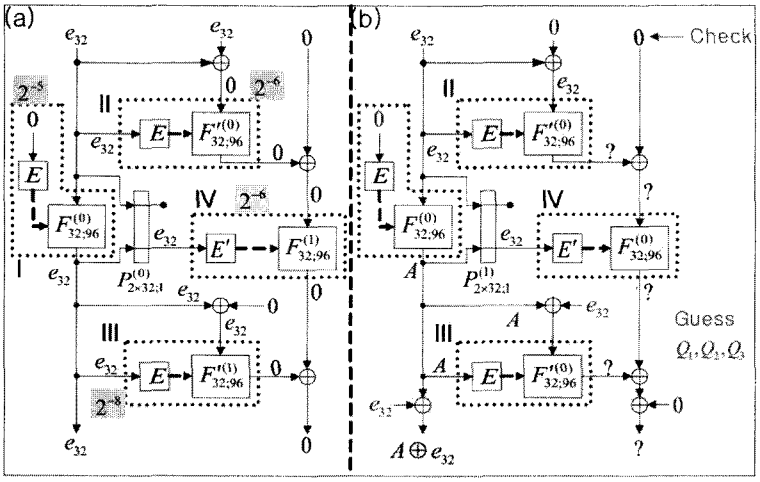
〔Table 4〕 Full-round related-key differential characteristic of SCO-1

Round (r)	ΔI_r	$\Delta K^{(1)}_r$	$\Delta G^{(1)}_r$	$\Delta T^{(1)}_r$	Part I				Part II				Part III				Part IV				Total
					ΔW	ΔX	ΔY	Pr.	ΔW	ΔX	ΔY	Pr.	ΔW	ΔX	ΔY	Pr.	ΔW	ΔX	ΔY	Pr.	Prob.
IT	$(0,0)$	·	e_{32}	0	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1
1	$(e_{32},0)$	0	e_{32}	0	0	e_{32}	e_{32}	2^{-5}	e_{32}	0	0	2^{-6}	e_{32}	e_{32}	0	2^{-8}	e_{32}	0	0	2^{-6}	2^{-25}
2	$(0,e_{32})$	0	0	e_{32}	0	0	0	1	0	0	0	1	0	e_{32}	e_{32}	2^{-5}	0	e_{32}	e_{32}	2^{-5}	2^{-10}
3	$(0,0)$	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1
4	$(0,0)$	e_{32}	0	0	e_{32}	0	0	2^{-6}	0	0	0	1	0	0	0	1	0	0	0	1	2^{-6}
5	$(0,0)$	e_{32}	0	0	e_{32}	0	0	2^{-6}	0	0	0	1	0	0	0	1	0	0	0	1	2^{-6}
6	$(0,0)$	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1
7	$(0,0)$	0	e_{32}	0	0	0	0	1	0	e_{32}	e_{32}	2^{-5}	0	0	0	1	0	e_{32}	e_{32}	2^{-5}	2^{-10}
8	$(e_{32},0)$	0	0	e_{32}	0	e_{32}	A	1	e_{32}	e_{32}	?	1	A	$A \oplus e_{32}$	?	1	e_{32}	?	?	1	1
FT	$(A,?)$	·	e_{32}	0	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1
Output	$(A \oplus e_{32}, ?)$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2^{-57}

$\Delta I_r = (\Delta I^L_r, \Delta I^R_r)$: the r-th round input difference.
Part I: $F^{(e_1)}_{32;96}(\Delta X, E(\Delta W)) = \Delta Y_{\text{Part I}}$, where $\Delta W = \Delta K^{(1)}_r$ and $\Delta X = \Delta I^L_r$.
Part II: $F^{(e_2)}_{32;96}(\Delta X, E(\Delta W)) = \Delta Y_{\text{Part II}}$, where $\Delta W = \Delta I^L_r$ and $\Delta X = \Delta I^L_r \oplus \Delta G^{(1)}_r$.
Part III: $F'^{(e_4)}_{32;96}(\Delta X, E(\Delta W)) = \Delta Y_{\text{Part III}}$, where $\Delta W = \Delta Y_{\text{Part I}}$ and $\Delta X = \Delta Y_{\text{Part I}} \oplus T^{(1)}_r$.
Part IV: $F^{(e_3)}_{32;96}(\Delta X, E'(\Delta W)) = \Delta Y_{\text{Part IV}}$, where $\Delta W = P^{e'}_{2\times 32;1}(\Delta I^L_r, \Delta Y_{\text{Part I}})$ and $\Delta X = \Delta I^R_r \oplus \Delta Y_{\text{Part II}}$.



[Fig. 4] The possible routes of $F^{(0)}_{32;96}(e_{32},0)$



[Fig. 5] (a) The first and (b) last round characteristics of SCO-1

difference $\Delta K = K \oplus K^* = (0, e_{32}, 0, 0)$. Our attack procedure is as follows.

1. Choose 2^{60} ciphertext pairs (C_j, C_j^*) with the difference $\alpha = (0,0)$ $(j = 1, \cdots, 2^{60})$. With a chosen ciphertext attack, (C_i, C_i^*) are decrypted using the keys K and K^*, respectively, to get the corresponding plaintext pairs (P_i, P_i^*).
2. Check that $P_i \oplus P_i^* = (A \oplus e_{32}, ?)$ for each i. We keep all plaintext pairs passing Step 2 in a table.
3. Guess a 64-bit subkey pair $((Q_1, Q_2), (Q_1^*, Q_2^*))$, where $Q_1^* = Q_1$, $Q_2^* = Q_2 \oplus e_{32}$, and do the followings;
   (1) Partially encrypt all plaintext pairs (P_i, P_i^*) passing Step 2 with the guessed subkey pair $((Q_1, Q_2), (Q_1^*, Q_2^*))$ to get the input pairs to Part I of the 8-th round. See [Fig. 5-(b)]. We denote these 32-bit pairs by (T_i, T_i^*). Check that $T_i \oplus T_i^* = e_{32}$ for each i.
   (2) Guess a 32-bit subkey pair (Q_3, Q_3^*), where $Q_3^* = Q_3$, and partially encrypt plaintext pairs passing Step 3-(1) to get the right half pairs of the input to the 8-th round. We denote these 32-bit pairs by (U_i, U_i^*). Finally, check that $U_i \oplus U_i^* = 0$ for each i.
   (3) If the number of pairs passing Step 3-(2) is greater than or equal to 6, go to Step 4. Otherwise, restart the above test with another

subkey pair.

4. For the suggested subkey pair, do an exhaustive search for the remaining 32-bit subkey Q_4 using trial decryption. During this procedure, if a 128-bit key satisfies two known plaintext and ciphertext pair, output this 128-bit key as the right 128-bit key of the full-round SCO-1. We also output the related key $K^* = K \oplus \Delta K$. Otherwise go to Step 3.

This attack requires 2^{60} ciphertext pairs and thus the data complexity of this attack is 2^{61} related-key chosen ciphertexts. Each plaintext pair can pass Step 2 with probability $2^{-26.42} (\approx 48 \cdot 2^{-32})$. So only $2^{33.58} (= 2^{60} \cdot 2^{-26.42})$ plaintext pairs pass Step 2. It follows that the required memory of this attack is about $2^{37.58} (= 2^{33.58} \cdot 2 \cdot 8)$ memory bytes.

The time complexity of Step 1 is 2^{61} full-round SCO-1 decryptions. The time complexity of Step 3-(1) is $2^{92.58} \left(\approx 2^{64} \cdot 2^{33.58} \cdot 2 \cdot \frac{1}{2} \cdot \frac{1}{8} \cdot \frac{1}{4} \right)$ full-round SCO-1 decryptions on average. Each plaintext pair can pass Step 3-(1) with probability $2^{-5.58} \left(\approx \frac{1}{48} \right)$. So the expected number of plaintext pairs passing Step 3-(1) is $2^{28} (\approx 2^{33.58} \cdot 2^{-5.58})$. Thus the time complexity of Step 3-(2) is $2^{120.59} \left(\approx 2^{96} \cdot 2^{28} \cdot 2 \cdot \frac{1}{2} \cdot \frac{1}{8} \cdot \frac{3}{4} \right)$. In order to estimate the time complexity of Step 4, we should check the expected number of wrong key pairs passing Step 3. The probability that a wrong subkey pair passes Step 3 is about $2^{-33.57} \left(\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-64})^i \cdot (1-(2^{-64}))^{t-i} \right) \right)$, where $t = 2^{60}$ represents the number of all possible plaintext pairs tested from Step 2. From the above analysis we expect that $2^{62.43} (\approx (2^{96}-1) \cdot 2^{-33.57})$ wrong subkey pairs pass Step 3 and Step 4 requires about $2^{94.43} (\approx 2^{32} \cdot 2^{62.43})$ full-round SCO-1 decryptions. Therefore the time complexity of this attack is about $2^{120.59} (\approx 2^{61} + 2^{92.58} + 2^{120.59} + 2^{94.43})$ full-round SCO-1 decryptions.

In Step 4, the probability that each 128-bit wrong key passes Step 4 is $2^{-128} (= 2^{-64 \cdot 2})$. It follows that the expected number of 128-bit wrong keys which pass Step 4 is $2^{-33.57} (= 2^{94.43} \cdot 2^{-128})$. Thus the possibility that the output of the above attack algorithm is a wrong key pair is very low. Moreover, the expected number of right pairs is about $8 (\approx 2^{60} \cdot 2^{-57})$ and the probability that the number of pairs suggested in Step 3 for the right subkey is no less than 6 is $0.81 \left(\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-57})^i \cdot (1-2^{-57})^{t-i} \right) \right)$, where $t = 2^{60}$. Therefore, with the success probability of 0.81, our related-key differential attack can break the full-round SCO-1.

Ⅳ. Conclusion

In this paper we have presented the first known cryptanalytic result of SCO-1 by using the related-key differential attack. As summarized in [Table 1], our attack on SCO-1 requires about $2^{120.56}$ time complexity smaller than the exhaustive search. This result implies that SCO-1 are still vulnerable to the related-key attack, though SCO-1 has been designed to advance conventional DDP-based ciphers which are vulnerable to the related-key attack.

References

[1] N. Goots, B. Izotov, A. Moldovyan and N. Moldovyan, "Modern cryptography: Protect Your Data with Fast Block Ciphers", *Wayne, A-LIST Publish.*, 2003.

[2] N. Goots, N. Moldovyan, P. Moldovyan and D. Summerville, "Fast DDP-Based Ciphers: From Hardware to Software", *46th IEEE Midwest International Symposium on Circuits and Systems*, 2003.

[3] N. Goots, A. Moldovyan, N. Moldovyan, "Fast Encryption Algorithm Spectr-H64", *MMM-ACNS'01*, LNCS 2052, pp. 275-286, Springer-Verlag, 2001.

[4] K. Jeong, C. Lee, J. Sung, S. Hong and J. Lim,

"Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128", *ACISP'07*, LNCS 4586, pp. 143-157, Springer-Verlag, 2007.

[5] Y. Ko, D. Hong, S. Hong, S. Lee and J. Lim, "Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property", *MMM-ACNS'03*, LNCS 2776, pp. 298-307, Springer-Verlag, 2003.

[6] Y. Ko, C. Lee, S. Hong and S. Lee, "Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1", *ACISP'04*, LNCS 3108, pp. 137-148, Springer-Verlag, 2004.

[7] Y. Ko, C. Lee, S. Hong, J. Sung and S. Lee, "Related-Key Attacks on DDP based Ciphers: CIKS-128 and CIKS-128H", *Indocrypt'04*, LNCS 3348, pp. 191-205, Springer-Verlag, 2004.

[8] C. Lee, D. Hong, S. Lee, S. Lee, H. Yang and J. Lim, "A Chosen Plaintext Linear Attack on Block Cipher CIKS-1", *ICICS'02*, LNCS 2513, pp. 456-468, Springer-Verlag, 2002.

[9] C. Lee, J. Kim, S. Hong, J. Sung and S. Lee, "Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b", *MYCRYPT'05*, LNCS 3715, pp. 245-263, Springer-Verlag, 2005.

[10] C. Lee, J. Kim, J. Sung, S. Hong and S. Lee, "Related-Key Differential Attacks on Cobra-H64 and Cobra-H128", *CCC'05*, LNCS 3796, pp. 201-219, Springer-Verlag, 2005.

[11] J. Lu, C. Lee and J. Kim, "Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b", *SCN'06*, LNCS 4116, pp. 95-110, Springer-Verlag, 2006.

[12] N. Moldovyan, "On Cipher Design Based on Switchable Controlled Operations", *MMM-ACNS'03*, LNCS 2776, pp. 316-327, Springer-Verlag, 2003.

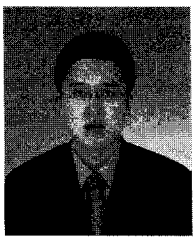
[13] A. Moldovyan and N. Moldovyan, "A cipher Based on Data-Dependent Permutations", *Journal of Cryptology*, Vol.15, No.1, pp. 61-72, 2002.

[14] N. Moldovyan, A. Moldovyan, M. Eremeev and N. Sklavos, "New Class of Cryptographic Primitives and Cipher Design for Networks Security", *International Journal of Network Security*, Vol.2, No.2, pp. 114-225, 2006.

[15] N, Moldovyan, A. Moldovyan, M. Eremeev and D. Summerville, "Wireless Networks Security and Cipher Design Based on Data-Dependent Operations: Classification of the FPGA Suitable Controlled Elements", *CCCT'04*, Vol.VII, pp. 123-128, Texas, USA, 2004.

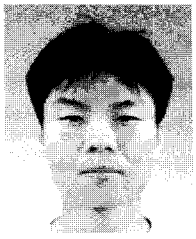
[16] N. Sklavos, N. Moldovyan and O. Koufopavlou, "High Speed Networking Security: Design and Implementation of Two New DDP-Based Ciphers", *Mobile Networks and Applications-MONET*, Kluwer Academic Publishers, Vol.25, Issue 1-2, pp. 219-231, 2005.

〈著者紹介〉

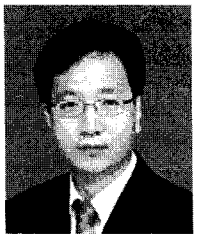


정 기 태 (Kitae Jeong) 학생회원
2004년 2월 : 고려대학교 수학과 학사
2006년 2월 : 고려대학교 정보보호대학원 석사
2006년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 블록 암호, 스트림 암호 및 해쉬 함수의 분석 및 설계

이 창 훈 (Changhoon Lee) 학생회원
2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2008년 2월 : 고려대학교 정보경영공학전문대학원 박사
2008년 3월~현재 : 고려대학교 정보경영공학전문대학원 연구교수
<관심분야> 대칭키 암호의 분석 및 설계



김 종 성 (Jongsung Kim) 정회원
2000년 8월 : 고려대학교 수학과 학사
2002년 8월 : 고려대학교 수학과 석사
2006년 11월 : K.U.Leuven 박사
2007년 2월 : 고려대학교 정보경영공학전문대학원 박사
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 연구교수
<관심분야> 대칭키 암호의 분석 및 설계



홍 석 희 (Seokhie Hong) 종신회원
1995년 2월 : 고려대학교 수학과 학사
1997년 2월 : 고려대학교 수학과 석사
2001년 2월 : 고려대학교 수학과 박사
1999년 8월~2004년 2월 : (주) 시큐리티 테크놀로지스 선임연구원
2004년 4월~2005년 2월 : K.U.Leuven 박사후연구원
2005년 3월~현재 : 고려대학교 정보경영공학전문대학원 조교수
<관심분야> 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식