한국항행학회 논문지 제13권 제6호 2009년 12월

# 블록 암호 SCOS-3의 연관키 차분 공격에 대한 안전성 분석

# Security Analysis of SCOS-3 Block Cipher against a Related-Key Attack

이창훈*

Chang-Hoon Lee*

## 요 약

최근, 하드웨어 환경에서 효율적으로 구현이 가능한 DDP, DDO, COS-기반 블록 암호에 대한 연구가 활발히 진행되고 있다. 그러나 대부분의 DDP, DDO, COS-기반 블록 암호들은 연관키 공격에 취약한 것으로 드러났다. 12-라운드 블록 암호 SCOS-3는 기제안된 DDP, DDO, COS의 취약점을 제거하기 위해 개발된 COS-기반 블록 암호이다. 본 논문에서는 SCOS-3의 11-라운드 축소 버전에 대한 연관키 차분 공격을 제안한다. 본 논문에서 소개하는 공격은 SCOS-3에 대한 첫 번째 공격이며, $2^{58}$개의 연관키 선택 평문을 이용하여 $2^{117.54}$의 11-라운드 SCOS-3 암호화 연산을 수행하여 11-라운드 SCOS-3의 비밀키를 복구한다. 이를 통해 SCOS-3가 여전히 연관키 공격에 취약함을 알 수 있다.

## Abstract

Recently, several DDP, DDO and COS-based block ciphers have been proposed for hardware implementations with low cost. However, most of them are vulnerable to related-keyt attacks. A 12-round block cipher SCOS-3 is desinged to eliminate the weakness of DDP, DDO and COS-based block ciphers. In this paper, we propose a related-key differential attack on an 11-round reduced SCOS-3. The attack on an 11-round reduced SCOS-3 requires $2^{58}$ related-key chosen plaintexts and $2^{117.54}$ 11-round reduced SCOS-3 encryptions. This work is the first known attack on SCOS-3. Therefore, SCOS-3 is still vulnerable to related-key attacks.

Key words : Block cipher, SCOS-3, Data-dependent operation, Related-key differential attack, Cryptanalysis

## I. 서 론

최근 하드웨어 환경에서 효율적으로 구현이 가능한 DDP(Data Dependent Permutation)와 DDO(Data Dependent Operation)-기반 블록 암호에 대한 연구가 활발히 진행되고 있고, 그 결과로서 다양한 블록 암호들이 제안되었다. 이 알고리즘들 매우 단순한 키스케줄을 사용하기 때문에, 비밀키가 빈번하게 변경되는 환경에 적용될 경우 높은 효율성을 갖는다. 그러나 대부분의 알고리즘들이 키스케줄의 취약점을 이용하는 공격인 연관키 공격에 취약한 것으로 드러났다 [2-9].

DDO와 DDP의 취약점을 제거할 수 있는 대안으로서, 출력 차분의 해밍 웨이트를 변화시킬 수 있는

* 한신대학교 공과대학 컴퓨터공학부(School of Computer Engineering, Hanshin University)
· 제1저자 (First Author) : 이창훈
· 투고일자 : 2009년 11월 10일
· 심사(수정)일자 : 2009년 11월 13일 (수정일자 : 2009년 12월 22일)
· 게재일자 : 2009년 12월 30일

COS(Controlled Operational Substitution)가 제안되었고 이를 기반으로 한 COS-기반 블록 암호 SCO- family가 제안되었다. SCO-family는 단순한 키스케줄을 사용하면서도 기존의 DDP와 DDO의 취약점을 제거할 수 있도록 설계되었다. 하지만 이 블록 암호 역시 연관키 공격에 취약한 것으로 드러났다 [1].

한편, COS-기반 블록 암호 SCOS-3는 기제안된 SCO-family의 하나인 SCO-3를 개선한 64-비트 블록 암호로서, 128-비트 비밀키를 사용한다. SCOS-3와 SCO-3는 매우 유사하다. 단지, SCOS-3는 SCO-3의 단순한 키스케줄로부터 야기될 수 있는 문제점들을 보완하기 위해 키스케줄을 변경하였다.

그렇지만, 본 논문에서는 수정된 키스케줄을 사용하는 11-라운드 축소 버전 SCOS-3도 여전히 연관키 차분 공격에 취약함을 보인다. 이 공격은 SCOS-3에 대한 첫 번째 공격이며, $2^{58}$개의 연관키 선택 평문을 이용하여 전수조사보다 작은 $2^{117.54}$의 11-라운드 SCOS-3 암호화 연산을 수행하여, 11-라운드 SCOS-3의 비밀키를 복구할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 SCOS-3와 이 블록 암호의 구조적인 성질을 간략히 소개하고, 3장에서는 11-라운드 SCOS-3에 대한 연관키 차분 공격을 소개한다. 마지막 4절에서는 결론을 맺는다.

## Ⅱ. SCOS-3

본 논문에서 비트 표기는 다음과 같다. 예를 들어, $P=(p_1,p_2,\cdots,p_n)$이면 $P$의 최상위 비트는 $p_1$이고, 최하위 비트는 $p_n$이다. 그리고 $e_{i,j}$는 $i$번째 비트와 $j$번째 비트만 1이고 나머지 비트는 0인 이진 수열을 의미한다. 예를 들어, $e_{1,3}=(1,0,1,\cdots,0)$이다.

### 2-1 COS-box

COS-box는 SCOS-3의 중요 구성 요소 중 하나이다. $e\in\{0,1\}$에 대하여, COS-box $F_{n;m}^{(e)}(X,V)$는 $n$-비트 $X$를 입력 받아 $m$-비트 제어 벡터 $V$를 이용하여 $n$-비트 $Y$를 출력한다. 그림 1과 같이, $F_{n;m}^{(e)}(X,V)$는 기본 블록 $F_{2;1}$을 결합하여 구성된다. 이때, $F_{2;1}$은 다음과 같이 정의된다.

$$F_{2;1}(x_1,x_2,v)=\big(x_1(v\oplus 1)\oplus x_2 v,\; x_1\oplus(x_2\oplus 1)(v\oplus 1)\big).$$

즉, $v=0$일 경우 $(y_1,y_2)=(x_1,x_1\oplus x_2\oplus 1)$이고, $v=1$일 경우 $(y_1,y_2)=(x_2,x_1)$이다.

그림 1에서 알 수 있듯이, $F_{n;m}^{(e)}$는 대칭적인 구조를 갖기 때문에 $F_{n;m}^{(0)}$과 역함수인 $F_{n;m}^{(1)}$은 $F_{2;1}$에 대한 제어 비트의 입력 순서만 다르고 나머지는 동일하다. 예를 들어, $V=(V_1,V_2,V_3)$이고 $V'=(V_3,V_2,V_1)$일 때 $F_{32;96}^{(0)}(\cdot,V)$와 $F_{32;96}^{(1)}(\cdot,V')$는 서로 역함수의 관계에 있다. 여기서 $F_{32;96}^{(e)}$에서 사용되는 치환 함수 $I_1$는 [10]를 참조하라.

그림 2와 같이, switchable COS-box $F_{n;m}^{(V,e)}$는 COS-box $F_{n;m}^{(e)}$와 CP(Controlled Permutation)-box $P_{m;1}^{(e)}$를 이용하여 구성된다. 예를 들어, $F_{32;96}^{(V,e)}$는 $F_{32;96}^{(e)}$과 $P_{96;1}^{(e)}$을 이용하여 구성된다. 이를 다음과 같이 표현할 수 있다: $F_{32;96}^{(V,e)}=F_{32;96}(X,V')$. 이때, $V'=P_{96;1}^{(e)}(V)$이다. 그림 2-(a)와 같이, $P_{96;1}^{(e)}$는 다음과 같이 계산된다. 여기서 $V_i$의 크기는 16비트이다.

$$P_{96;1}^{(0)}(V_1,V_2,V_3,V_4,V_5,V_6)=(V_1,V_2,V_3,V_4,V_5,V_6),$$
$$P_{96;1}^{(1)}(V_1,V_2,V_3,V_4,V_5,V_6)=(V_6,V_5,V_4,V_3,V_2,V_1).$$

### 2-2 SCOS-3

블록 암호 SCOS-3는 128-비트 비밀키 $Q=(Q_1,Q_2,Q_3,Q_4)$를 사용하는 64-비트 블록 암호로서 라운드 수는 12이다. SCOS-3의 라운드 함수인 $Crypt^{(e)}$는 그림 3과 같다. 여기서 $e=0(1)$은 암호화(복호화) 과정을 의미한다. 표 1은 SCOS-3의 12-

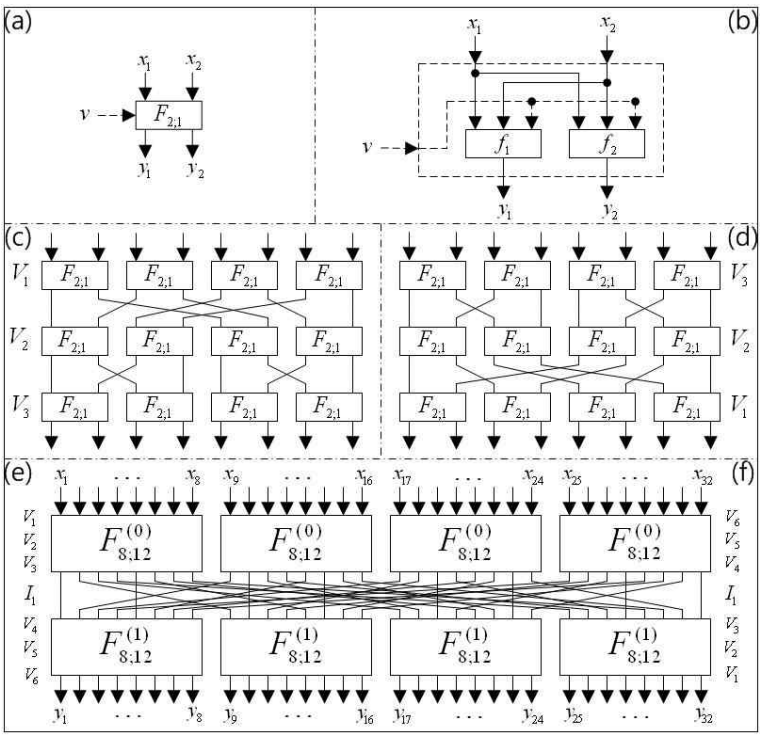

그림 2. (a)$F_{2;1}$ (b)$F_{2;1}$ (c)$F_{8;12}^{(0)}$ (d)$F_{8;12}^{(1)}$ (e)$F_{32;96}^{(0)}$ (f)$F_{32;96}^{(1)}$
Fig. 2. (a)$F_{2;1}$ (b)$F_{2;1}$ (c)$F_{8;12}^{(0)}$ (d)$F_{8;12}^{(1)}$ (e)$F_{32;96}^{(0)}$ (f)$F_{32;96}^{(1)}$

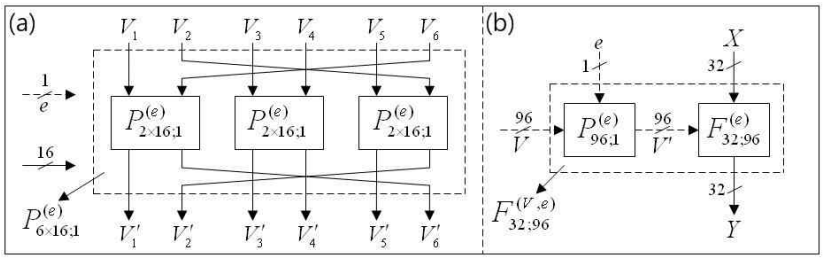

그림 3. (a) $P_{96;1}^{(e)}$-box (b) $F_{32;96}^{(V;e)}$-box
Fig. 3. (a) $P_{96;1}^{(e)}$-box (b) $F_{32;96}^{(V;e)}$-box

라운드 암호화 과정($e=0$)을 나타낸 것이다. 복호화 과정에서 $P$, $G_r^{(0)}$, $T_r^{(0)}$은 $C$, $G_r^{(1)}$, $T_r^{(1)}$로 각각 바뀐다. 제어 벡터를 생성하는데 사용되는 extension box $E$는 [10]을 참조하라.

COS-box $F_{32;96}^{(e_i)}$ $(i=1,2,3,4)$는 그림 1과 같이 $F_{2;1}$을 사용하여 구성된다. 제어 비트 $e'$에 대하여, $P_{2\times 32;1}^{(e')}(x_1,x_2)$는 두 개의 32-비트 입력값 $x_1,x_2$를 사용하여 다음과 같이 두 개의 32-비트 출력값 $y_1,y_2$를 생성한다.

$$P_{2\times 32;1}^{(e')}(x_1,x_2)=\big(e'(x_1\oplus x_2)\oplus x_1,\; e'(x_1\oplus x_2)\oplus x_2\big)$$

즉, $e'=0$일 경우 $(y_1,y_2)=(x_1,x_2)$이고 $e'=1$일 경우 $(y_1,y_2)=(x_2,x_1)$이다.

SCOS-3의 키 스케줄은 매우 단순하다. 128-비트 비밀키 $Q=(Q_1,Q_2,Q_3,Q_4)$가 바로 $Crypt^{(e)}$에 사용된다. 표 2는 SCOS-3의 라운드 키와 매개변수 $e'$을 나타낸 것이다.

표 1. SCOS-3의 암호화 과정
Table 1. 블록암호 SCOS-3

(1) 64-비트 평문 블록 $P$ 는 두 개의 서브 블록 $P_L$과 $P_R$로 나뉜다.
(2) $(A,B)\leftarrow(P_L,P_R)$.
(3) $r=1$ 부터 $r=11$이 될 때까지 $r$값을 1씩 증가시키며, 다음 과정을 수행한다.
  - $(A,B)\leftarrow Crypt^{(0)}\left(A,B,G_r^{(0)},T_r^{(0)}\right)$. 여기서, $G_r^{(0)}$와 $T_r^{(0)}$는 $r$번째 라운드 키들이다.
  - 두 개의 서브블록을 서로 교환한다. : $(A,B)\leftarrow(B,A)$;
(4) $(A,B)\leftarrow Crypt^{(0)}\left(A,B,G_{12}^{(0)},T_{12}^{(0)}\right)$.
(5) 최종 치환과정을 수행한다; $(A,B)\leftarrow\left(A\boxminus G_{FT}^{(0)},B\boxplus T_{FT}^{(0)}\right)$.
(6) $(C_L,C_R)\leftarrow(A,B)$.
(7) $C=(C_L,C_R)$을 암호문으로 출력한다.

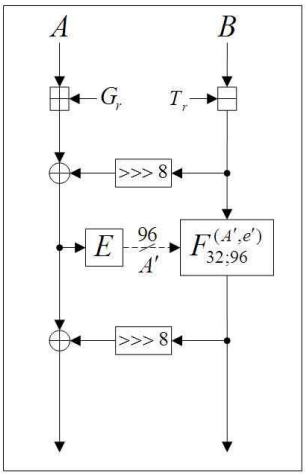


그림 3. 라운드 함수 $Crypt^{(e)}$
Fig. 3. The round function $Crypt^{(e)}$

## Ⅲ. 11-라운드 SCOS-3에 대한 연관키 차분 공격

본 장에서는 11-라운드 SCOS-3에 대한 연관키 차분 공격을 제안한다. 본 장에서 소개하는 SCOS-3에 대한 연관키 공격은 [1]에서 제안된 11-라운드 SCO-3에 대한 연관키 공격과 매우 유사하다. 서론에서 언급한 바와 같이, SCOS-3는 연관키 공격에 취약한 SCO-3를 개선한 블록 암호이다. 하지만 SCO-3와 SCOS-3는 키스케줄을 제외하고 동일한 구조를 갖는다. 또한 11-라운드 SCO-3에 대한 연관키 공격에서 사용한 연관키 차분 특성이 SCOS-3에 동일하게 적용된다. 이는 SCOS-3의 변경된 키스케줄이 연관키 공격에 대한 안전성을 증가시키지 못함을 의미한다.

표 2. SCOS-3의 라운드 키와 매개변수 $e'$
Table 2. The specification of parameter $e'$ and round keys of SCOS-3

| Round $r$ | $e=0$ | | | $e=1$ | | |
|---|---|---|---|---|---|---|
| | $G_r^{(0)}$ | $T_r^{(0)}$ | $e'$ | $G_r^{(1)}$ | $T_r^{(1)}$ | $e'$ |
| 1 | $Q_1$ | $Q_2$ | 1 | $Q_2$ | $Q_3$ | 1 |
| 2 | $Q_3$ | $Q_4$ | 0 | $Q_4$ | $Q_1$ | 0 |
| 3 | $Q_3$ | $Q_2$ | 1 | $Q_2$ | $Q_3$ | 0 |
| 4 | $Q_4$ | $Q_1$ | 0 | $Q_1$ | $Q_4$ | 1 |
| 5 | $Q_4$ | $Q_3$ | 1 | $Q_1$ | $Q_3$ | 0 |
| 6 | $Q_1$ | $Q_2$ | 1 | $Q_2$ | $Q_4$ | 0 |
| 7 | $Q_4$ | $Q_3$ | 0 | $Q_3$ | $Q_4$ | 0 |
| 8 | $Q_4$ | $Q_2$ | 0 | $Q_2$ | $Q_1$ | 0 |
| 9 | $Q_3$ | $Q_1$ | 1 | $Q_3$ | $Q_4$ | 1 |
| 10 | $Q_4$ | $Q_1$ | 1 | $Q_1$ | $Q_4$ | 0 |
| 11 | $Q_3$ | $Q_2$ | 1 | $Q_2$ | $Q_3$ | 1 |
| 12 | $Q_1$ | $Q_4$ | 0 | $Q_4$ | $Q_3$ | 0 |
| FT | $Q_2$ | $Q_3$ | • | $Q_1$ | $Q_2$ | • |

공격 환경은 다음과 같다. 평문 쌍 $P=(P_L,P_R)$과 $P^*=(P_L^*,P_R^*)$를 비밀키 $K$, $K^*$로 각각 암호화한다고 가정한다. 이때 평문 쌍과 비밀키는 $\alpha=P\oplus P^*=(0,e_1)$와 $\Delta K=K\oplus K^*=(e_1,e_1,e_1,e_1)$을 만족한다. 그러면 그림 4-(a)와 같이, SCOS-3에 대한 확률 $2^{-6}$의 1-라운드 연관키 차분 특성 $\alpha\rightarrow\beta=(0,e_1)$를 구성할 수 있다.

1-라운드 연관키 차분 특성의 확률 $2^{-6}$은 다음과 같이 계산된다. 입력 차분이 $\Delta X$이고 제어 벡터 차분이 $\Delta V$일 때, $\Pr_{(COS')}(\Delta Y/\Delta X)$를 $COS'\in\left\{F_{32;96}^{(\Delta V,0)},F_{32;96}^{(\Delta V,1)}\right\}$의 출력 차분이 $\Delta Y$일 확률로 정의한다. 그러면 다음을 만족한다.

$$\Pr_{\left(F_{32;96}^{(E(e_1),0)}\right)}(0/0)) = \Pr_{\left(F_{32;96}^{(E(e_1),1)}\right)}(0/0)) = 2^{-6}$$

위의 식은 다음과 같은 식에 의해 계산된다. 여기서, $\Pr_{(F_{2;1})}(\Delta Y/\Delta X, \Delta V)$와 $\Pr_{(COS)}(\Delta Y/\Delta X, \Delta V)$는 $F_{2;1}$의 출력 차분이 $\Delta Y$일 확률과 $COS \in \{F_{32;96}^{(0)}, F_{32;96}^{(1)}\}$의 출력 차분이 $\Delta Y$일 확률을 각각 의미한다.

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

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

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

(4) $\Pr_{(F_{32;96}^{(0)})}(0/0, E(e_1)) = \Pr_{(F_{32;96}^{(1)})}(0/0, E(e_1)$ $E(e_1)) = 2^{-6}$, where $E(e_1) = (e_3, e_5, e_9, 0, 0, 0)$.

이 차분 특성을 반복 적용하여, 확률 $2^{-54}$의 9-라운드 연관키 차분 특성 $\alpha \rightarrow \beta$를 구성할 수 있다.

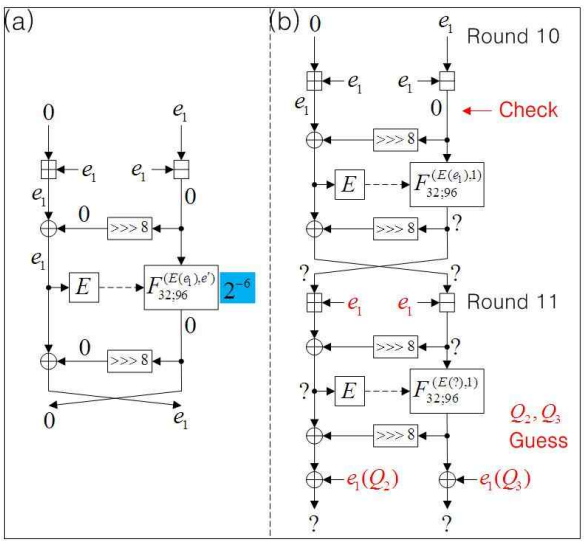


그림 5. (a) 1-라운드에 대한 차분 특성
(b) 11-라운드 SCOS-3에 대한 공격 과정
Fig. 5. (a) The first round characteristic of SCOS-3
(b) The attack procedure on an 11-round SCOS-3

9-라운드 연관키 차분 특성을 이용하여 11-라운드 SCOS-3에 대한 연관키 차분 공격을 수행한다. SCOS-3가 $\Delta K = K \oplus K^* = (e_1, e_1, e_1, e_1)$을 만족하는 비밀키 $K$와 연관키 $K^*$를 사용한다고 가정할 때, 11-라운드 SCOS-3에 대한 연관키 차분 공격은 다음과 같은 과정을 수행한다.

(1) 차분 $\alpha = (0, e_1)$을 만족하는 $2^{57}$개의 평문 쌍 $(P_j, P_j^*)$를 선택한다 $(j = 1, \cdots, 2^{57})$. 선택 평문 공격 가정 하에서, $(P_i, P_i^*)$를 비밀키 $K$, $K^*$로 각각 암호화하여 암호문 쌍 $(C_i, C_i^*)$을 생성하고 테이블에 저장한다.

(2) $Q_2^* = Q_2 \oplus e_1$와 $Q_3^* = Q_3 \oplus e_1$을 만족하는 64-비트 부분키 쌍 $((Q_2, Q_3), (Q_2^*, Q_3^*))$를 추측하여 다음을 수행한다;

(가) 추측한 부분키 쌍 $((Q_2, Q_3), (Q_2^*, Q_3^*))$를 이용하여 라운드 10에서 라운드 키 덧셈 부분의 출력값을 각각 계산한다 (그림 5-(b) 참조). 이 64-비트 값을 $(T_i, T_i^*)$라 할 때, 각각의 $i$에 대해 $T_i \oplus T_i^* = (e_1, 0)$을 만족하는지 검사한다.

(나) 단계 2-(1)을 통과하는 암호문 쌍의 개수가 6 이상이면, 단계 3으로 간다. 그렇지 않으면 단계 2로 간다.

(3) 단계 2를 통과한 부분키 쌍에 대하여, 나머지 64-비트 부분키 $(Q_1, Q_4)$을 전수조사하고 2개의 평문/암호문 쌍을 이용하여 검사한다. 2개의 평문/암호문 쌍을 만족하는 128-비트 비밀키를 11-라운드 SCOS-3의 옳은 128-비트 비밀키로 출력하고 연관키 $K^* = K \oplus \Delta K$도 출력한다. 그렇지 않으면 단계 2로 간다.

이 공격을 수행하기 위해 $2^{57}$개의 평문 쌍이 필요하므로 이 공격의 데이터 복잡도는 $2^{58}$개의 연관키 선택 평문이다. 그리고 이 공격에 필요한 메모리는 $2^{61}(= 2^{57} \cdot 2 \cdot 8)$ 메모리 바이트이다.

단계 1의 계산 복잡도는 $2^{58}$ 11-라운드 SCOS-3 암호화 연산이고, 단계 2-(1)의 계산 복잡도는 평균 $2^{117.54}(\approx 2^{64} \cdot 2^{57} \cdot 1/2 \cdot 2/11)$ 11-라운드

SCOS-3 암호화 연산이다. 틀린 부분키 쌍이 단계 2-(2)를 통과할 확률은 다음과 같다. 여기서 $t = 2^{57}$은 모든 암호문 쌍의 수를 의미한다.

$$2^{-51.42}\left(\approx \sum_{i=6}^{t}\left(\binom{t}{i} \cdot (2^{-64})^i \cdot (1-(2^{-64}))^{t-i}\right)\right)$$

그래서 평균적으로 약 $2^{11.58}(\approx (2^{64}-1) \cdot 2^{-51.42} \cdot 1/2)$개의 틀린 부분키 쌍이 단계 2-(2)를 통과하고 단계 3의 계산 복잡도는 $2^{75.48}$ $(\approx 2^{64} \cdot 2^{11.58})$ 11-라운드 SCOS-3 암호화 연산이다. 그러므로 이 공격 알고리즘의 계산 복잡도는 약 $2^{117.54}(\approx 2^{58}+2^{117.54}+2^{75.48})$ 11-라운드 SCOS-3 암호화 연산이다.

한편, 각각의 128-비트 틀린 키가 단계 3을 통과할 확률은 $2^{-128}(=2^{-64 \cdot 2})$이고 그래서 $2^{-52.52}$ $(=2^{75.48} \cdot 2^{-128})$개의 틀린 키가 단계 3을 통과한다. 이는 본 논문에서 제안하는 공격 알고리즘이 틀린 키 쌍을 출력할 확률이 매우 낮음을 의미한다. 게다가, $2^{57}$개의 암호문 쌍 중에서 앞에서 소개한 차분 경로를 통해 생성된 암호문 쌍의 개수의 기댓값은 $8(=2^{57} \cdot 2^{-54})$이고 옳게 추측한 부분키에 대하여 단계 2-(1)을 통과하는 암호문 쌍의 개수가 6 이상일 확률은 다음과 같다 $(t = 2^{57})$.

$$0.81(\approx \sum_{i=6}^{t}\left(\binom{t}{i} \cdot (2^{-54})^i \cdot (1-2^{-54})^{t-i}\right)\right)$$

그러므로 0.81의 성공 확률로 본 논문에서 제안하는 연관키 차분 공격은 11-라운드 SCOS-3의 128-비트 비밀키를 복구할 수 있다.

## Ⅳ. 결 론

본 논문에서는 COS-기반 블록 암호 SCOS-3의 11-라운드 축소 버전에 대한 연관키 차분 공격을 제안하였다. 본 논문에서 소개한 공격을 이용하여 전수조사 보다 효율적인 $2^{117.54}$의 계산 복잡도로 11-라운드 SCOS-3의 비밀키를 복구할 수 있다. 이를 통해, SCOS-3가 연관키 공격에 취약한 SCO-3 블록 암호를 개선하기 위해 설계되었지만, 여전히 연관키 공격에 취약함을 알 수 있다.

## 감사의 글

이 논문은 한신대학교 학술연구비 지원에 의하여 연구되었음

## 참 고 문 헌

[1] K. Jeong, C. Lee, J. Kim and S. Hong, “Security analysis of the SCO-family using key schedules”, Information Sciences, Vol. 179, Issue 24, pp. 4232-4242, Elsevier, 2009.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] N. Moldovyan, A. Moldovyan and M. Eremeev, "A Class of Data-Dependent Operations", International Journal Network Security, Vol. 2, No. 3, pp. 187-204, 2006.

## 이 창 훈 (李昌勳)

2001년 02월 : 한양대학교 자연과학부 수학전공(이학사)

2003년 02월 : 고려대학교 정보보호전문대학원(공학석사)

2008년 02월 : 고려대학교 정보경영공학전문대학원 정보보호전공(공학박사)

2009년 03월~현재 : 한신대학교 컴퓨터공학부 전임강사

2009년 03월~현재 : 한국정보처리학회 영어논문지 JIPS 편집위원

2009년 09월~현재 : 국제학술저널 IJITCC 편집위원

관심분야 : 정보보호, 암호학, 디지털포렌식 등