# 블록암호 SEED-192에 대한 취약키 분석

# Analysis for Weak Keys of the Block Cipher SEED-192

김종성*, 조기조*

Jong-Sung Kim*, Ki-Jo Cho*

요 약

본 논문에서는 블록암호 SEED-192 키 스케줄 취약점을 분석한다. 본 연구 결과에 의하면, SEED-192는 전체 20 라운드 중 16 라운드에 대해, 연관키 렉탱글/부메랑 공격에 대한 취약키가 존재한다. 이는 SEED-192 키 스케줄에 대한 최초의 분석 결과이다.

Abstract

In this paper, we analyze the key schedule of the block cipher SEED-192. According to the result of this paper, there exist weak keys in 16 out of 20 rounds of SEED-192 against the related-key rectangle/boomerang attack. This is the first cryptanalytic result for the key schedule of SEED-192.

Key words : Block Cipher, SEED-192, Weak Keys, Related-key Boomerang Attack

## I. 서 론

과거, 블록암호는 국방 또는 외교와 같은 국가 기밀을 위해 주로 사용되었다. 하지만, 1976년 DES[9]를 미연방 표준 블록암호로 채택한 이후, 블록암호는 국가 기밀 이외에 민간에서 필요한 정보보호 서비스를 제공하는 핵심 기술로 사용되고 있다. DES가 미연방 표준 블록암호로 채택된 이후, 블록암호에 대한 연구는 DES에 대한 취약점 분석 연구가 주를 이루었다. DES의 취약점 분석 결과, DES는 키에 대한 전수조사 공격에 안전하지 않음이 밝혀졌다. 미국 NIST에서는 안전하지 못한 DES를 대체할 필요성을 느끼고, 2000년도에 새로운 미연방 표준 블록암호 AES[10]를 선정하였다.

AES는 키 길이 128, 192 또는 256 비트를 지원하는데, 128, 192 비트 키를 사용하는 AES는 민간용 정보보호기술에 주로 사용되고, 256 비트 키를 사용하는 AES는 국방 또는 외교와 같은 국가 기밀을 위해 사용되고 있다. 한편, 국내에서 개발한 SEED[1]의 경우, 128 비트 키만을 지원하였지만, 최근, AES와 같이 다양한 어플리케이션 환경에 사용될 수 있도록 192, 256 비트 키를 지원하는 키 스케줄 알고리즘이 개발되었다. 하지만, 최근 개발된 SEED-192[2], SEED-256[2] 키 스케줄 알고리즘에 대한 안전성 검증이 충분히 이루어지지 않은 상태이다.

본 논문에서는 SEED-192의 키 스케줄 알고리즘에 대한 안전성을 평가한다: 본 연구는 SEED-192 전체 20 라운드 중 16 라운드에 대해, 연관키 렉탱글/부메랑 공격에 대한 취약키가 존재함을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는

* 경남대학교 e-비즈니스학부(Division of e-Business, Kyungnam University)
· 제1저자 (First Author): 김종성 교신저자 (Corresponding Author): 조기조
· 투고일자 : 2011년 1월 20일
· 심사(수정)일자 : 2011년 1월 21일 (수정일자 : 2011년 2월 22일)
· 게재일자 : 2011년 2월 28일

SEED-192 알고리즘을 소개한다. 3장에서는 SEED-192 키 스케줄 알고리즘에 대한 안전성 분석을 다룬다. 4장은 본 논문의 결론이다.

## Ⅱ. 블록암호 SEED-192

본 장에서는 SEED-192의 암호화 알고리즘을 소개하고 (복호화 과정은 암호화 과정의 역순이므로 생략함), SEED-192의 키 스케줄 알고리즘을 소개한다. 본 장의 알고리즘 소개는 [2]의 내용을 인용하였다.

### 2-1. 암호화 알고리즘

암호화 알고리즘의 전체 구조는 그림 1과 같이 Feistel 구조로 이루어져 있으며, 128-비트 평문 $(L^0, R^0)$과 192-비트 비밀키 $K$를 사용하여, 총 20 라운드를 거쳐 128-비트 암호문 $(L^{16}, R^{16})$을 출력한다.

본 장에서는 다음과 같은 표기를 사용한다.

- o $a \boxplus b$: $(a+b) \bmod 2^{32}$
- o $a \| b$: $a$와 $b$의 논리곱
- o $X^{\lll s}(X^{\ggg s})$: $X$를 $s$ 비트만큼 왼쪽(오른쪽)으로 순환 이동하는 연산
- o $(L^i, R^i)$: 128-비트 라운드 $i$의 출력값
- o $K^i = (K_0^i, K_1^i)$: 라운드 $i$의 64-비트 라운드 키
- o $X = (X_3 \| X_2 \| X_1 \| X_0)$: $G$ 함수의 32-비트 입력값
- o $Y = (Y_3 \| Y_2 \| Y_1 \| Y_0)$: $G$ 함수에서 S-box $(S_1, S_2)$의 32-비트 출력값
- o $m_i$: 상수
- o $KC_i$: 키 스케줄에서 사용되는 라운드 $i+1$의 라운드 상수

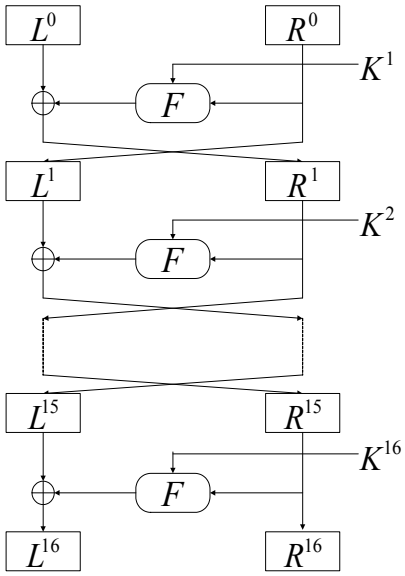


그림 1. SEED-192 암호화 알고리즘
Fig. 1. Encryption algorithm of SEED-192

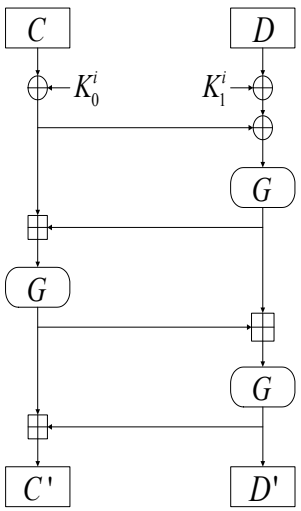


그림 2. $F$ 함수
Fig. 2. $F$ function

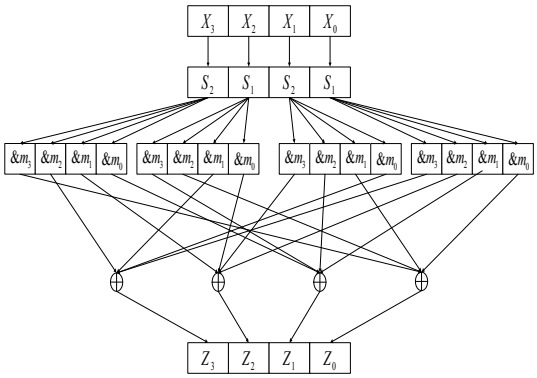

그림 3. $G$ 함수
Fig. 3. $G$ function

$F$ 함수는 그림 2와 같이 64-비트 $(C,D)$와 라운드 키 $K^i=\left(K_0^i,K_0^i\right)$을 입력 받아서 64-비트 출력값 $(C',D')$를 생성한다. 여기서 $i$는 라운드 수를 의미한다.

$G$ 함수는 그림 3과 같이 32-비트 $X$를 입력 받아서 32-비트 출력값 $Z(=Z_3\|Z_2\|Z_1\|Z_0)$를 생성한다. $G$ 함수를 수식으로 표현하면 다음과 같다. $m_0=0xfc,\ m_1=0xf3,\ m_2=0xcf,\ m_3=0x3f.$

$$Y_3=S_2(X_3), Y_2=S_1(X_2), Y_1=S_2(X_1), Y_0=S_1(X_0)$$
$$Z_3=(Y_0\wedge m_3)\oplus(Y_1\wedge m_0)\oplus(Y_2\wedge m_1)\oplus(Y_3\wedge m_2),$$
$$Z_2=(Y_0\wedge m_2)\oplus(Y_1\wedge m_3)\oplus(Y_2\wedge m_0)\oplus(Y_3\wedge m_1),$$
$$Z_1=(Y_0\wedge m_1)\oplus(Y_1\wedge m_2)\oplus(Y_2\wedge m_3)\oplus(Y_3\wedge m_0),$$
$$Z_0=(Y_0\wedge m_0)\oplus(Y_1\wedge m_1)\oplus(Y_2\wedge m_2)\oplus(Y_3\wedge m_3).$$

$G$ 함수의 내부에 사용되는 비선형 S-box $S_1,S_2$는 다음의 식을 이용하여 생성된다 (여기서 $n_1=247,\ n_2=251,\ b_1=159,\ b_2=56$이다).

$$S_i: Z_{2^8}\rightarrow Z_{2^8},\ S(x)=A^{(i)}\cdot x^{n_i}\oplus b_i$$

$$A^{(1)}=\begin{pmatrix}1&0&0&0&1&0&1&0\\1&1&1&1&1&1&1&0\\1&0&0&0&0&1&0&1\\0&1&0&0&0&0&1&0\\0&1&0&0&0&1&0&1\\0&0&1&0&0&0&0&1\\1&0&0&0&1&0&0&0\\0&0&0&1&0&1&0&0\end{pmatrix},\quad A^{(2)}=\begin{pmatrix}0&1&0&0&0&1&0&1\\1&0&0&0&0&1&0&1\\1&1&1&1&1&1&1&0\\0&0&1&0&0&0&0&1\\1&0&0&0&1&0&1&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\end{pmatrix}$$

## 2-2. 키 스케줄 알고리즘

SEED-192의 키 스케줄은 192-비트 비밀키 $K$를 입력 받아 그림 4와 같은 과정을 수행하여 20 라운드에 대한 각 라운드 키를 생성한다. 주어진 192-비트 비밀키 $K$를 6개의 32-비트 레지스터 $A,B,C,D,E,F$에 다음과 같이 저장한다: $K=A\|B\|C\|D\|E\|F$. 각 라운드 $r$에 사용되는 라운드 키 $K^r=(K_0^r,K_1^r)$은 그림 4와 같은 방식으로 생성된다. 그림 4에서 순환 이동 수 $rot$는 9, 8, 12를 번갈아 사용한다. $KC_r$은 라운드 상수이다.

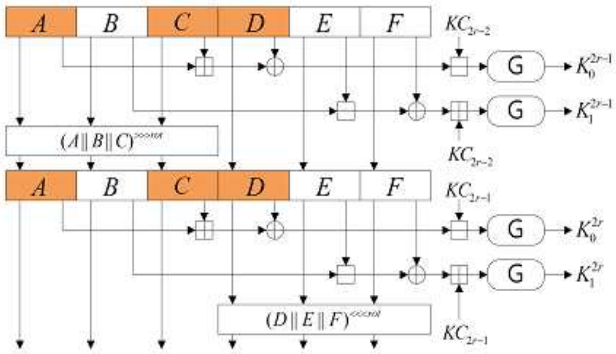


그림 4. SEED-192 키 스케줄
Fig. 4. Key schedule of SEED-192

## Ⅲ. 키 스케줄을 이용한 SEED-192 공격

취약키 공격[5]과 연관키 공격[3]은 키 스케줄을 이용하는 분석법이다. 블록암호에 취약키를 사용하는 경우 다른 키를 사용할 때 보다 특정 공격에 블록암호의 안전도가 떨어지게 된다. [5]에 의하면, IDEA에는 부메랑 공격에 안전하지 못한 여러 취약키가 존재한다. 연관키 공격은 블록암호에 연관키가 사용되었을 때 적용되는 일종의 차분 공격으로, 1993년 Biham에 의해 연관키 공격[3]이 소개된 이후, 연관키 렉탱글 공격, 연관키 부메랑 공격[4,6,7] 등 여러 연관키 변형 공격이 발표되었다. 또한, 취약키 공격과 연관키 공격을 합성한 취약키 공간을 이용한 연관키 공격도 발표되었다[8].

본 장에서는 SEED-192의 축소 라운드에 대한 취약키 공간을 이용한 연관키 공격 및 연관키 렉탱글/

부메랑 공격을 소개한다.

다음은 본 장에서 사용하는 기호이다.

o $\Delta X$: 레지스터 $X$에 대한 비트별 xor 차분 ($X = A, B, C, D, E, F, G$ or $H$)

o $x_i$: 레지스터 $X$의 $i$번째 비트 값 ($i = 0,1,\cdots,31$: $x_0$인 경우, $X$의 가장 오른쪽 위치의 비트 값으로 가장 작은 값의 비트를 의미하고, $x_{31}$인 경우, $X$의 가장 왼쪽 위치의 비트 값으로 가장 큰 값의 비트를 의미함)

o $\Delta X = e^{i,j}$: $\Delta X$의 $i$, $j$번째 비트 값은 1이고 나머지 비트들은 모두 0임

한 라운드 키를 생성하기 위해 SEED-192 키 스케줄은 두 개의 $G$ 함수를 라운드 키 생성 바로 전 단계에 적용한다. 두 번째 $G$ 함수의 입력값 $((B-E)\oplus F)+Cst$와 $G$ 함수의 출력값의 차분 성질을 살펴보자(여기서, $Cst$는 상수값임).

Fact 1. $\Delta B = 0$, $B = 2^{32}-1$, $\Delta E = \Delta F$이면, $\Delta(B-E) = \Delta E$, $\Delta((B-E)\oplus F) = \Delta E \oplus \Delta F = 0$가 된다. 따라서, 라운드 키 생성시 사용되는 두 번째 $G$ 함수의 출력차분은 0이다. 즉, $\Delta G(((B-E)\oplus F)+Cst) = 0$.

또한, $(A\|B\|C)$와 $(D\|E\|F)$ 각각에 로테이션 양을 9, 8, 12를 번갈아가며 사용하기 때문에, 누적 로테이션 양을 다음 Fact 2와 같이 얻을 수 있다.

**Fact 2**. 라운드 키 생성시 누적 로테이션 양은 다음과 같다.

| $r$ | $r$ 라운드 키 생성시 $(A\|B\|C)$의 오른쪽 누적 로테이션 양 | $r$ 라운드 키 생성시 $(D\|E\|F)$의 왼쪽 누적 로테이션 양 |
|---|---|---|
| 1 | 0 | 0 |
| 2 | 9 | 0 |
| 3 | 9 | 9 |
| 4 | 17 | 9 |
| 5 | 17 | 17 |
| 6 | 29 | 17 |
| 7 | 29 | 29 |
| 8 | 38 | 29 |
| 9 | 38 | 38 |
| 10 | 46 | 38 |
| 11 | 46 | 46 |
| 12 | 58 | 46 |
| 13 | 58 | 58 |
| 14 | 67 | 58 |
| 15 | 67 | 67 |
| 16 | 75 | 67 |
| 17 | 75 | 75 |
| 18 | 87 | 75 |
| 19 | 87 | 87 |
| 20 | 0 | 87 |

다음은 SEED-192의 키 스케줄에 관한 차분 성질이다.

**Property 1.** 키 $K = A\|B\|C\|D\|E\|F$와 연관키 $K' = A'\|B'\|C'\|D'\|E'\|F'$의 차분 $\Delta K = 0\|0\|0\|0\|\Omega\|\Omega$ ($\Omega \in S, S = \{e^0, e^1, e^2, e^{0,1}, e^{0,2}, e^{1,2}, e^{0,1,2}\}$)와 $A = B = 2^{32}-1, c_0 = c_1 = c_2 = c_3 = c_4 = c_5 = 1$이면, 첫 번째 라운드 키부터 여덟 번째 라운드 키 차분 모두 0이 된다. 즉, $\Delta K^1 = \Delta K^2 = \cdots = \Delta K^8 = 0$이다.

**(증명)** Property 1은 라운드 1-8의 라운드 키 생성 시 사용되는 두 개의 $G$ 함수 각각의 입력 차분이 모두 0이 됨을 보임으로써 증명할 수 있다. 우선, $\Delta A = \Delta B = \Delta C$이고, Fact 2에 의해 $(D\|E\|F)$의 로테이션 양이 8 라운드까지 32를 넘지 못함으로 각 라운드 키 생성 시 첫 번째 $G$ 함수의 입력 차분이 0이 된다. 키 생성 시 두 번째 $G$ 함수의 입력에 사용되는 레지스터는 $B, E, F$이다. $\Delta E = \Delta F$이고 이 두 차분은 S 집합의 원소이다. 또한, 8 라운드까지 $(D\|E\|F)$의 누적 로테이션 양이 29이므로 $\Delta E, \Delta F$의 1 차분의 비트 위치는 8 라운드까지 각각 레지스터 $E, F$를 벗어나지 못한다. 또한, 두 번째 $G$ 함수의 입력은 상수부분을 제외하면 $(B-E)\oplus F$이 된다. 따라서, Fact 1에 의해 $B-E$의 차분과 $F$의 차분이 동일하면, 두 번째 $G$ 함수의 입력 차분은 0이 된다. 각 라운드 키 생성시 사용된 로테이션 양을 고려하면,

$A=B=2^{32}-1, c_0=c_1=c_2=c_3=c_4=c_5=1$와 $\Delta E=\Delta F\in S$에 의해 $\Delta K^1=\Delta K^2=\cdots=\Delta K^8=0$. ∎

Property 1을 이용하여 확률 1을 갖는 다음의 8 라운드 연관키 특성을 꾸밀 수 있다.

**Proposition 1. [8 라운드 연관키 특성]** 키 $K=A\|B\|C\|D\|E\|F$와 $K'=A'\|B'\|C'\|D'\|E'\|F'$의 성질이

$\Delta K=0\|0\|0\|0\|\Omega\|\Omega$,($\Omega\in S, S$는 Property 1참조)와 $A=B=2^{32}-1, c_0=c_1=c_2=c_3=c_4=c_5=1$

을 만족한다고 가정하자. 그러면, 확률 1인 8 라운드 연관키 차분 특성 0→0 가 존재한다(라운드 1-8).

**(증명)** Property 1에 의해 $\Delta K^1=\Delta K^2=\cdots=\Delta K^8=0$이 된다. 따라서, 평문 차분이 0이면 8 라운드 후의 출력 차분 또한 0이 된다. ∎

위와 비슷한 방법으로 라운드 9-16에 대한 8 라운드 연관키 특성 또한 찾을 수 있다.

**Property 2.** 키 $K=A\|B\|C\|D\|E\|F$와 연관키 $K'=A'\|B'\|C'\|D'\|E'\|F'$의 차분 $\Delta K=0\|0\|0\|\Omega'\|\Omega'\|0$ ($\Omega'\in T, T=\{e^{26}, e^{27}, e^{28}, e^{26,27}, e^{26,28}, e^{27,28}, e^{26,27,28}\}$)와 $a_6=a_7=\cdots=a_{31}=b_0=b_1=\cdots=b_{10}=1$, $C=2^{32}-1$이면, 아홉 번째 라운드 키부터 열여섯 번째 라운드 키 차분 모두 0이 된다. 즉, $\Delta K^9=\Delta K^{10}=\cdots=\Delta K^{16}=0$이다.

**(증명)** 키 스케줄에서 9 번째 라운드 키를 생성하기 위해 사용되는 레지스터 값의 왼쪽 96비트는 $(A\|B\|C)^{\gg 38}$이고, 오른쪽 96비트는 $(D\|E\|F)^{\ll 38}$이다. 만약 $\Delta D=\Delta E\in T$, $\Delta F=0$이면, $\Delta(D\|E\|F)^{\ll 38}=0\|\Omega\|\Omega$ ($\Omega\in S, S$는 Property 1참조)이 된다. 또한, $a_6=a_7=\cdots=a_{31}=b_0=b_1=\cdots=b_{10}=1$, $C=2^{32}-1$의 값은 $(A\|B\|C)^{\gg 38}$를 거친 이후의 상태 값 $A=B=2^{32}-1, c_0=c_1=c_2=c_3=c_4=1$로 변환된다. 따라서, Property 1의 증명 방식에 의해 $\Delta K^9=\Delta K^{10}=\cdots=\Delta K^{16}=0$이 된다 (Property 1의 $c_5$에 대한 조건이 빠진 이유는 라운드 9-16에 사용되는 로테이션 양은 8, 12, 9, 8인 반면, 라운드 1-8에 사용되는 로테이션 양이 9, 8, 12, 9이기 때문이다). ∎

위 성질을 이용하여 확률 1을 갖는 다음의 8 라운드 연관키 특성을 꾸밀 수 있다.

**Proposition 2. [8 라운드 연관키 특성]** 키 $K=A\|B\|C\|D\|E\|F$와 연관키 $K'=A'\|B'\|C'\|D'\|E'\|F'$의 성질이

$\Delta K=0\|0\|0\|\Omega'\|\Omega'\|0$,($\Omega'\in T, T$는 Property 2참조)와 $a_6=a_7=\cdots=a_{31}=b_0=b_1=\cdots=b_{10}=1, C=2^{32}-1$

을 만족한다고 가정하자. 그러면, 확률 1인 8 라운드 연관키 차분 특성 0→0 가 존재한다(라운드 9-16).

**(증명)** Property 2에 의해 $\Delta K^9=\Delta K^{10}=\cdots=\Delta K^{16}=0$이 된다. 따라서, 9 라운드 입력 차분이 0이면 16 라운드 후의 출력 차분 또한 0이 된다. ∎

Propostions 1, 2를 이용한 취약키 공간에서의 연관키 렉탱글/부메랑 공격에 대해 살펴보자. 연관키 렉탱글/부메랑 공격은 두 개의 서브 사이퍼에 대한 연관키 특성을 결합하여 분석한다. 본 연구에서는 첫 번째 서브 사이퍼에 대한 연관키 특성을 위해 Proposition 1을, 두 번째 서브 사이퍼에 대한 연관키 특성을 위해 Proposition 2를 이용한다. 16 라운드에 대한 취약키 공간을 이용한 연관키 렉탱글/부메랑 특성은 Theorems 1, 2와 같다.

**Theorem 1. [16 라운드 연관키 렉탱글 특성]** 키 차분 $\Delta K=0\|0\|0\|0\|\Omega\|\Omega$, ($\Omega\in S, S=\{e^0, e^1, e^2, e^{0,1}, e^{0,2}, e^{1,2}, e^{0,1,2}\}$)이고, 또 다른 키 차분 $\Delta K'=0\|0\|0\|\Omega'\|\Omega'\|0$, ($\Omega'\in T, T=\{e^{26}, e^{27}, e^{28}, e^{26,27}, e^{26,28}, e^{27,28}, e^{26,27,28}\}$)을 만족한다고 가정하자.

키 $K1$의 첫 번째 세 워드가 $A=B=C=2^{32}-1$

의 값을 갖는다고 가정할 때, $K1$의 연관키 $K2 = K1 \oplus \Delta K, K3 = K1 \oplus \Delta K', K4 = K1 \oplus \Delta K \oplus \Delta K'$에 대해 다음의 성질을 만족한다.

"16 라운드 암호화 과정을 $Enc$로 표시하고, $Enc_{K1}(P) = C1$, $Enc_{K2}(P) = C2$, $Enc_{K3}(P') = C3$, $Enc_{K4}(P') = C4$라 할 때, 확률 $2^{-128}$으로 $C1 \oplus C3 = C2 \oplus C4 = 0$을 만족한다."

**(증명)** $Enc1$을 처음 8 라운드 암호화 과정으로, $Enc2$를 마지막 8 라운드 암호화 과정으로 표기하자. 그러면, Proposition 1에 의해 $Enc1_{K1}(P) = Enc1_{K2}(P)$, $Enc1_{K3}(P') = Enc1_{K4}(P')$을 만족한다. 만약 $Enc1_{K1}(P) = Enc1_{K3}(P')$이면(이를 만족할 확률은 약 $2^{-128}$임), $Enc1_{K2}(P) = Enc1_{K4}(P')$이 된다. $X = Enc1_{K1}(P) = Enc1_{K3}(P')$, $Y = Enc1_{K2}(P) = Enc1_{K4}(P')$로 표기하면, Proposition 2에 의해, $Enc2_{K1}(X) = Enc2_{K3}(X)$, $Enc2_{K2}(Y) = Enc2_{K4}(Y)$를 만족한다. 즉, $C1 \oplus C3 = C2 \oplus C4 = 0$이다. 따라서, $C1 \oplus C3 = C2 \oplus C4 = 0$를 만족할 확률은 $2^{-128}$이다. 랜덤 사이퍼에 대해, 이 성질을 만족할 확률은 $2^{-256}$이다. ∎

**Theorem 2. [16 라운드 연관키 부메랑 특성]** 키 $K1$ $(A = B = C = 2^{32} - 1)$와 연관키 $K2 = K1 \oplus \Delta K, K3 = K1 \oplus \Delta K'$, $K4 = K1 \oplus \Delta K \oplus \Delta K'$에 대해 다음의 성질을 만족한다. ($\Delta K, \Delta K'$은 Theorem 1 참조).

"16 라운드 암호화 과정을 $Enc$로, 16 라운드 복호화 과정을 $Dec$로 표시하고, $Enc_{K1}(P) = C1$, $Enc_{K2}(P) = C2$라 할 때, 확률 1로 $Dec_{K3}(C1) = Dec_{K4}(C2)$을 만족한다."

**(증명)** $Dec_{K3}(C1) = P1, Dec_{K4}(C2) = P2$라고 하자. 그러면, $P1 = P2$를 보이면 된다. Proposition 1에 의해 $Enc1_{K1}(P) = Enc1_{K2}(P)$이며, Proposition 2에 의 해 , $Enc1_{K3}(P1) = Enc1_{K1}(P), Enc1_{K4}(P2) = Enc1_{K2}(P)$가 된다. 즉, $Enc1_{K3}(P1) = Enc1_{K4}(P2)$이다. 따라서, Proposition 1에 의해 $P1 = P2$가 성립한다. ∎

## Ⅳ. 결 론

본 논문에서는 SEED-192 키 스케줄에 대한 안전성을 분석하였다. 본 연구 결과에 의하면, SEED-192의 8 라운드에 대해 취약키 공간을 이용한 연관키 특성이 존재하며, SEED-192의 16 라운드에 대해 취약키 공간을 이용한 연관키 렉탱글, 부메랑 특성이 존재한다. 본 논문의 결과는 SEED-192 키 스케줄에 대한 최초의 분석 결과이다.

## 감사의 글

이 연구결과물은 2010학년도 경남대학교 학술연구장려금 지원에 의한 것임

## 참 고 문 헌

[1] 한국정보보호진흥원, "128비트 블록암호 알고리즘 (SEED) 개발 및 분석 보고서", 2003.

[2] 한국정보보호진흥원, "블록암호 알고리즘 SEED-192/256 개발", 2008.

[3] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys", *Journal of Cryptology,* Vol. 7, No. 4, pp. 229-246, Springer-Verlag, 1994.

[4] E. Biham, O. Dunkelman and N. Keller, "Related-Key Boomerang and Rectangle Attacks", *EUROCRYPT'05, LNCS 3494,* pp. 507-525, Springer- Verlag, 2005.

[5] A. Biryukov, J. Nakahara J., B. Preneel, J. Vandewalle, "New Weak-Key Class of IDEA", *ICICS'02, LNCS 2513*, pp. 315-326, Springer-Verlag, 2002.

[6] J. Kim, S. Hong and B. Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", *FSE'07, LNCS 4593,* pp. 225-241, Springer-Verlag, 2007.

[7] J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, "The

Related-Key Rectangle Attack - Application to SHACAL-1", *ACISP'04, LNCS 3108, pp. 123-136, Springer-Verlag,* 2004.

[8] E. Lee, J. Kim, D. Hong, C. Lee, J. Sung and S. Hong, "Weak-Key Classes of 7-Round MISTY 1 and 2 for Related-Key Amplified Boomerang Attacks", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,* Vol. E91-A, No. 2, pp. 642-649, 2008.

[9] National Bureau of Standards, "Data Encryption Standard", *Federal Information Processing Standards Publication 46*, Jan. 1977.

[10] National Institue of Standards and Technology, "Advanced Encryption Standard", *Federal Information Processing Standards Publications*, No. 197, 2001.

## 김 종 성 (金宗星)

2000년 8월 : 고려대학교 수학과 (이학사)
2002년 8월 : 고려대학교 수학과 (이학석사)
2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC (공학박사)
2007년 2월: 고려대학교 정보보호 대학원 (공학박사)
2007년 3월 ~ 2009년 8월 : 고려대학교 정보보호기술 연구센터 연구교수
2009년 9월 ~ 현재 : 경남대학교 e-비즈니스학부 전임강사
관심분야 : 블록암호, 해쉬함수, 디지털 포렌식

## 조 기 조 (曺基祚)

1981년 2월 : 경남대학교 경영학부 (경영학사)
1983년 8월 : 부산대학교 경영학과 (경영학석사)
1989년 8월 : 동아대학교 경영학과 (경영학박사)
1986년 9월 ~ 현재 : 경남대학교 e-비즈니스학부 정교수
관심분야 : 정보보호, 정보시스템 감사