情報保護學會論文誌
第20卷 第4號, 2010. 8

7-라운드 SEED에 대한 향상된 차분 공격*

성 재 철†
서울시립대학교

Improved Differential Attack of Seven-Round SEED*

Jaechul Sung†
University of Seoul

요 약

블록 암호알고리즘 SEED 국내 TTA(정보통신기술협회)와 더불어 국제 ISO/IEC 표준으로 사용되고 있는 128비트 입출력을 갖는 국내에서 개발된 알고리즘이다. SEED 개발 이후 현재까지 알려진 가장 좋은 공격 방법은 2002년 Yanami 등이 제안한 차분 분석 방법이다. 이 공격 방법은 확률 2^{-124}의 6-라운드 차분 특성을 이용하여, 7-라운드 SEED를 2^{127}의 데이터 복잡도로 분석하였다. 본 논문에서는 확률 2^{-110}의 새로운 6-라운드 새로운 차분 특성을 제시하고, 이를 이용하여 7-라운드 SEED를 2^{113}의 데이터 복잡도로 공격할 수 있음을 보인다.

ABSTRACT

Block Cipher SEED which was developed by KISA are not only Korea national standard algorithm of TTA but also one of standard 128-bit block ciphers of ISO/IEC. Since SEED had been developed, many analyses were tried but there was no distinguishing cryptanalysis except the 7-round differential attack in 2002. The attack used the 6-round differential characteristic with probability 2^{-124} and analyzed the 7-round SEED with 2^{127} chosen plaintexts. In this paper, we propose a new 6-round differential characteristic with probability 2^{-110} and analyze the 7-round SEED with 2^{113} chosen plaintexts.

Keywords: Block cipher, SEED, Related-Key Attacks, Weak-Key Classes

I. 서 론

블록 암호에 대한 가장 강력한 분석 방법은 차분 공격으로, DES가 차분 공격으로 분석된 이후 다수의 알고리즘들이 차분 분석 방법으로 많이 분석되었다.[2,6,7] 이러한 차분 공격이 개발된 이후, 차분 및 선형 분석에 증명 가능한 안전성을 제시하는 구조에 대해서도 많은 연구가 진행되었다.[1,4] 또한 블록 암호의 키스케줄의 특성과 차분 특성을 결합한 연관 키 공격 및 연관 암호 공격 등을 이용한 다양한 분석 방법들도 제시되었다.[3,5]

ISO/IEC의 128-비트 블록 암호 표준으로는 AES, Camellia, SEED가 있다.[8,9,11] AES는 NIST의 AES 프로젝트에 의해 채택된 벨기에의 알고리즘이고, Camellia는 일본에서 개발되었고, SEED는 1999년 대한민국 KISA에서 개발된 알고리즘이다.

SEED는 16-라운드 DES와 같은 Feistel 구조를 가지는 블록 암호알고리즘이다. SEED가 개발된 이후 국내 뿐 아니라 전 세계적으로 다양한 분석이 시도되었으나 뚜렷한 연구 분석 결과는 제시되지 못한 실정이다. 다만 2002년 H. Yanami와 T. Shimoyama가 제시한 7 라운드에 대한 공격이 유일한 분석 방법으로 알려져 있다.[12]

이 공격 방법은 가장 기본 적인 차분 분석 방법으로

* 접수일(2010년 3월 15일), 게재확정일(2010년 6월 7일)
* 이 논문은 2010년도 서울시립대학교 연구년교수 연구비에 의하여 연구되었음
† 주저자 : jcsung@uos.ac.kr

〔표 1〕 7-라운드 SEED 공격

	데이터 복잡도	계산 복잡도	6-라운드 차분특성 확률
Yanami et al. [12]	2^{127}	$2^{124.19}$	2^{-124}
본 논문	2^{113}	$2^{110.19}$	2^{-110}

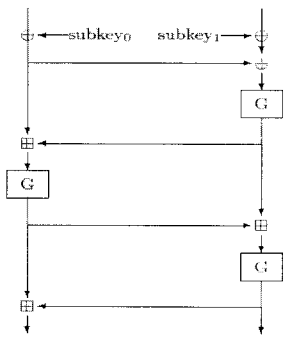
확률 2^{-124}을 가지는 6-라운드 차분 특성을 이용하여 한 라운드를 덧붙이는 1R 공격을 하였다. 따라서 7-라운드 SEED를 2^{126}개의 평문-암호문 쌍, 즉 2^{127}의 데이터 복잡도로 공격한 방법이다. H. Yanami와 T. Shimoyama의 이 공격 방법은 개발자가 제시한 6-라운드 최대 차분 특성 확률인 2^{-130}보다 높은 확률을 갖는 특성을 법 2^{32}에서의 덧셈 특성을 이용해 찾은 것이다.

본 논문에서는 확률 2^{-124}을 가지는 6-라운드 차분 특성보다 좋은 새로운 6-라운드 특성을 제시한다. 이 차분 특성의 확률은 기존의 차분 특성 확률보다 2^{14}배 좋은 것으로, 이를 이용하면 7-라운드 SEED의 복잡도를 2^{127}에서 2^{113}으로 낮출 수 있다.

II. 블록 암호 SEED 소개

블록 암호의 구조는 크게 DES와 같은 Feistel 구조와 AES와 같은 SPN 구조로 나눌 수 있다. 블록 암호알고리즘 SEED는 DES와 같은 Feistel 구조이고, 128-비트의 입출력을 갖는다. SEED는 키 사이즈는 현재 128-비트만을 사용하고 있다.

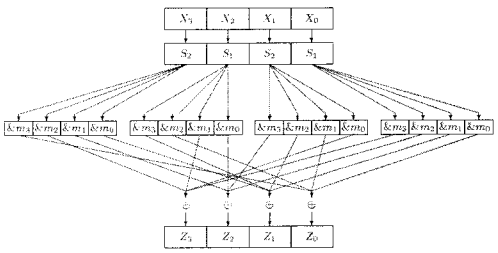
SEED의 라운드 함수 F는 64-비트의 입출력을 갖는 함수로 변형된 3-라운드 MISTY 구조이다. 라운드 함수에는 총 64-비트의 키가 사용된다. 이 3-라운드 MISTY 구조는 차분 및 선형 관점에서 실제적인 안전성을 제공할 뿐 아니라 의사난수 과점에서 이론적인 안전성을 제공하는 구조이다.



〔그림 1〕 SEED의 라운드 함수 F

라운드 함수 F에 사용된 G 함수는 32-비트의 입출력을 갖는 함수로 차분 및 선형 공격의 측면에서 좋은 특성을 지닌 함수이다. G 함수에는 라운드 키는 사용되지 않는다.

다음 그림은 SEED의 라운드 함수 F에 사용되는 G 함수를 나타낸 것이다. 여기서 $m_0 = fc_x$, $m_1 = f3_x$, $m_2 = cf_x$, $m_3 = 3f_x$이다. 차분 분석 관점에서의 SEED의 G 함수는 branch number가 4라는 특성을 가지고 있다.



〔그림 2〕 SEED의 G 함수

본 논문의 공격의 SEED의 키 스케줄의 특성을 이용하지 않으므로 소개는 생략한다.

III. 기존 7-라운드 차분 분석

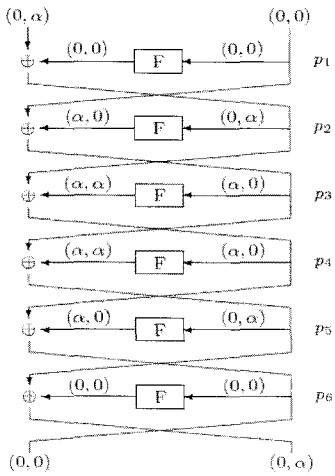
본 절에서는 2002년 H. Yanami와 T. Shimoyama가 제시한 지금까지 알려진 SEED 가장 좋은 차분 특성을 소개한다.[12] SCN2002의 논문에서는 라운드 함수의 좌우가 바뀐 잘못된 그림을 이용하여 차분 특성을 설명하였다. 이는 그림의 좌우만 바뀐 것으로 안전성 분석 및 이론에는 직접적인 영향은 없다. 다만 표기를 바로잡기 위해 본 논문에서는 올바른 라운드 함수 그림을 이용하여 H. Yanami와 T. Shimoyama를 바로 잡아 표기할 것이다. 또한, 여기서 표기하는 수는 모두 16진법을 이용하여 표기한다.

3.1. 기존의 6-라운드 차분 특성

다음의 그림은 논문 [12]에서 제시한 가장 좋은 6-라운드 차분 특성이다. 여기서, $\alpha = 80000080_x$이다.

이 차분 특성의 확률 p는 다음과 같다.

$$p = p_1p_2p_3p_4p_5p_6 = 1 \cdot 2^{-31} \cdot 2^{-31} \cdot 2^{-31} \cdot 2^{-31} \cdot 1 = 2^{-124}.$$



〔그림 3〕 기존의 6-라운드 차분 특성

자세한 각각의 p_i의 확률 및 각 라운드의 차분 특성은 본 논문에서는 생략한다. 자세한 내용은 논문을 참고하길 바란다.[12]

H. Yanami와 T. Shimoyama는 앞서 제시한 차분 특성과 함께 확률이 두 번째로 높은 또 다른 차분 특성도 제시하였다. 하지만, 이 두 번째 차분 특성의 확률은 2^{-128}로 랜덤 특성의 확률과 같아 실제적인 차분 분석에는 사용될 수 없는 특성이다.

3.2. 6-라운드 차분 특성을 이용한 7-라운드 공격

앞서 제시한 확률 2^{-124}의 6-라운드 차분 특성을 이용한 7-라운드 공격은 다음과 같다.

단계 0 (데이터 수집 과정)
- $2^{126}(=4\cdot 2^{124})$ 평문 쌍 (P, P^*)에 대한 암호문 쌍 (C, C^*)을 얻는다.

단계 1 (키 초기화 과정)
- 마지막 7번 째 라운드 후보 키 2^{64}개를 초기화 한다.

단계 2 (잘못된 쌍 필터링 과정)
- 암호문 쌍 (C, C^*)에 대해, 오른 쪽 반의 차분이 (00000000, 80000080)이 아닌 쌍을 버린다.

단계 3 (후보 쌍을 이용한 키 카운트 과정)
- 단계 2에서 남은 암호문 쌍을 이용하여, 7-라운드 키 후보에 대해 7-라운드 함수의 64-비트 출력 차분과 암호문의 왼쪽 차분의 XOR한 값이 (00000000, 00000000)이 되는 지를 체크한 후, 값을 만족한 경우 키 후보를 1씩 증가시킨다.

단계 4 (후보 쌍을 이용한 키 카운트 과정)
- 단계 3의 키 카운트 중 가장 높이 카운트 되는 키를 올바른 키로 출력한다.

7-라운드 공격은 가장 전형적인 차분 공격 기법이다. H. Yanami와 T. Shimoyama의 논문에서는 계산 복잡도 및 성공 확률에 대한 명확한 언급이 생략되었다. 본 논문에서의 위의 각 단계별 복잡도 및 확률을 엄밀히 살펴보자.

우선, 단계 0은 데이터를 수집하는 단계로 총 2^{126}개의 평문 쌍에 대한 암호문 쌍이 필요하다. 즉, 2^{127}개의 평문에 대한 암호문이 필요하다. 또한, 단계 1에서는 총 2^{64}개의 64-비트 메모리가 필요하다.

단계 2에서는 잘못된 쌍(wrong pair)을 필터링하는 과정으로 필터링 확률이 2^{-64}이므로, 총 2^{126}개의 쌍 중 평균적으로 2^{62}개의 쌍만이 남는다.

단계 3은 남은 2^{62}쌍을 가지고, 2^{64}개의 키 후보에 대해 라운드 함수 연산을 하여야 한다. 즉 $2^{124.19}\,(=2\cdot 2^{62}\cdot 2^{64}\cdot \frac{1}{7})$의 계산 복잡도가 필요하다. 여기서 단위는 7-라운드 SEED 암호화이다.

하지만, 단계 3의 계산 복잡도는 라운드 함수 F에 대해 사전 테이블을 미리 계산한 후 저장 해 두면 복잡도를 낮출 수 있다. 즉, 라운드 함수 F에서 라운드 키가 XOR 된 후의 값과 출력 값을 미리 계산해 놓은 것이다. 이렇게 사전에 이러한 테이블을 미리 계산 해 놓으면 2^{127}번의 XOR와 테이블 look-up 연산으로 계산 가능하다. 물론 2^{127}번의 XOR와 테이블 look-up 연산이 $2^{124.19}$ 7-라운드 SEED 암호화 연산보다 효과적이어야 한다. 단계 3을 이렇게 구성할 경우, 추가의 2^{64}의 64-비트 메모리가 더 필요하다.

마지막 단계 4의 성공 확률을 살펴보자. 잘못된 키에 대해 키가 카운트되는 것에 대한 분포를 포아송 분포 $X\sim Poi(\lambda)$를 따른다고 가정하자. 그러면, 올바른 키의 경우 $\lambda = M1 = 4$이고, 잘못된 키가 카운트 되는 경우는 평균 $\lambda = M2 = 2^{-2}$이 된다. 따라서 threshold를 어떻게 잡느냐에 따라 옳은 키가 포함될 성공 확률 $\Pr[X_{M1}\geq k]$과 잘못된 키가 포함된 확률 $\Pr[X_{M2}\geq k]$이 달라진다. 일반적으로 $k=4$로 놓고, 두 확률을 계산하면 다음과 같다.

$$\Pr[X_{M1} \geq 4] = 0.000133 = 2^{-12.87}. \quad (1)$$

$$\Pr[X_{M2} \geq 4] = 0.57. \quad (2)$$

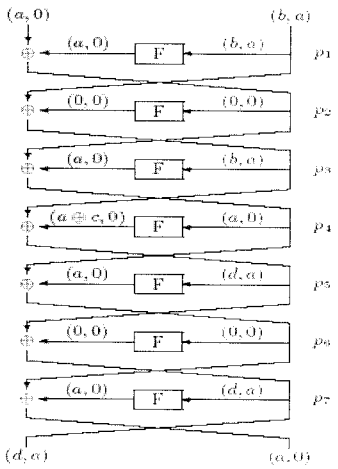
확률 (1)은 잘못된 키 중 $2^{-12.87}$의 확률로 살아남는 다는 뜻이고, (2)는 올바른 키 후보가 이 안에 있을 확률이 0.57 정도가 된다는 것을 의미한다.

IV. 새로운 7-라운드 차분 분석

본 절에서는 앞서 제시한 6-라운드 차분 특성보다 확률이 높은 새로운 차분 특성을 제시하고, 이를 이용한 공격 방법을 소개한다. 기본적인 정의 및 기호는 [12]의 논문을 사용한다. 물론 앞의 경우와 같이 차분은 비트별 XOR 차분을 사용한다.

4.1. 새로운 6-라운드 차분 특성

다음은 새로운 6-라운드 차분 특성을 그림으로 나타낸 것이다.



[그림 4] 새로운 6-라운드 차분 특성

위의 그림에서, a,b,c,d는 32-비트의 0이 아닌 차분을 나타내고 $a \oplus b \oplus c \oplus d = 0$을 만족한다. 이 새로운 차분 특성 식의 확률 $p\,(= p_1 p_2 p_3 p_4 p_5 p_6)$를 계산하자. 우선 $p_2 = p_6 = 1$이다. 또한, 첫 번째 라운드와 세 번째 라운드의 특성식이 같으므로 $p_1 = p_3$이다. 확률은 다음과 같이 정의된다. 따라서 확률은 $p = p_1^2 p_4 p_5$이다.

앞의 SEED의 라운드 함수의 그림에서 라운드 키가 XOR되는 부분은 XOR 차분에 영향을 주지 않으므로 이를 제거한 라운드 함수의 차분을 살펴본다. 확률 $p_1 \cdot p_4, p_6$의 값이 크고, $a \oplus b \oplus c \oplus d = 0$을 만족하는 a,b,c,d의 값을 얻기 위해서는 라운드 함수의 차분 특성의 변화를 잘 살펴보아야 한다. 라운드 함수의 차분에서 가장 민감하게 영향을 주는 것은 다음 두 가지이다.

함수 G의 active S박스 수 (a)

XOR 차분의 덧셈 (b)

우선, 라운드 함수 F는 있는 세 개의 G 함수에서 최소의 active S박스의 수는 2이다. 또한 덧셈 부분의 확률을 최대화하기 위해서는 비트별 0이 아닌 차분의 수가 적어야 한다. 이러한 사항들을 고려하여 우리는 다음 두 가지의 a,b,c,d의 값을 찾았다.

[표 2] 두 개의 가능한 a,b,c,d의 값

	TYPE 1	TYPE 2
a	80808000_x	80808000_x
b	87808000_x	83808000_x
c	00808000_x	00808000_x
d	07808000_x	03808000_x

TYPE 1과 TYPE 2는 b와 d의 1-비트만 제외하고 같은 값이다. 우선 TYPE1의 경우의 세 개의 라운드 함수 F에 대한 차분 특성 및 확률을 살펴보자. 다음은 첫 번째 라운드의 차분 특성을 나타낸 것이다.

첫 라운드의 차분 특성 확률을 살펴보자. 라운드 함수 F의 차분 특성의 확률은 $p_1 = q_1 q_2 q_3 q_4 q_5 q_6$이다. 각 q_i는 다음과 같이 정의된다.

$$q_1 = \Pr[07000000_x \xrightarrow{G} 80808000_x] = \Pr[07_x \xrightarrow{S_2} 80_x] = 2^{-6}.$$

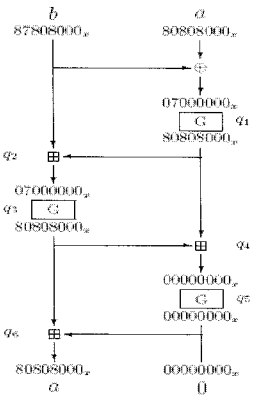
$$q_2 = \Pr[(87808000_x, 80808000_x) \xrightarrow{+} 07000000_x] = 2^{-5}.$$

$$q_3 = \Pr[07000000_x \xrightarrow{G} 80808000_x] = \Pr[07_x \xrightarrow{S_2} 80_x] = 2^{-6}.$$

$$q_4 = \Pr[(80808000_x, 80808000_x) \xrightarrow{+} 00000000_x] = 2^{-2}.$$

$$q_5 = \Pr[00000000_x \xrightarrow{G} 00000000_x] = 1.$$

$$q_6 = \Pr[(80808000_x, 00000000_x) \xrightarrow{+} 80808000_x] = 2^{-2}.$$



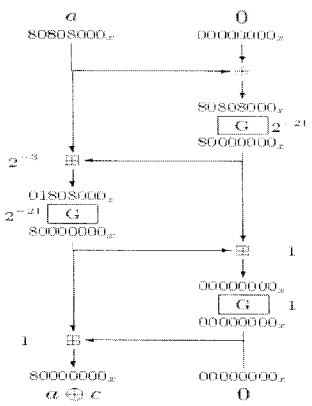
〔그림 5〕 F 차분 특성 I : $(b,a)\rightarrow(a,0)$

여기서 G 함수에 대한 확률은 S_1및 S_2의 차분 분포표를 이용하면 쉽게 계산되고, 덧셈에 대한 확률은 덧셈과 XOR의 차분의 변화에 대한 연구들을 이용하면 된다.[10,12] 따라서 $p_1 = 2^{-21}$이다.

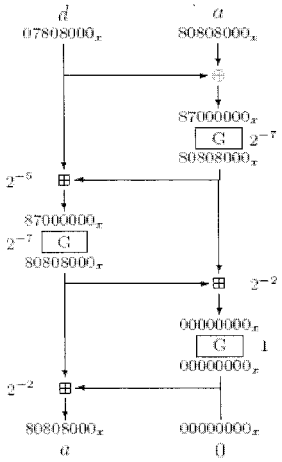
다음의 〔그림 6〕과 〔그림 7〕은 4-라운드 및 5-라운드의 차분 특성을 나타낸 것이다. 이 두 개의 차분 특성의 확률도 앞의 방법을 동일하게 적용하면, $p_4 = 2^{-45}$이고 $p_5 = 2^{-23}$이다.

따라서 TYPE 1의 6-라운드 차분 특성의 확률 $p = p_1^2 p_4 p_5 = (2^{-21})^2 \cdot 2^{-45} \cdot 2^{-23} = 2^{-110}$이 된다.

TYPE 2의 경우도 거의 비슷한 방법으로 확률을 계산하면, $p_1 = 2^{-22}$, $p_4 = 2^{-45}$, $p_5 = 2^{-22}$이 된다. 따라서 6-라운드 차분 특성 확률은 $p = p_1^2 p_4 p_5 = 2^{-111}$이 된다. TYPE 1의 경우가, TYPE 2보다 라운드 차분 특성 I에서 차분 특성의 확률이 큰 것은 $\Pr[07 \xrightarrow{S_2} 80] = 2^{-6}$의 확률이 $\Pr[03 \xrightarrow{S_2} 80] = 2^{-7}$보다 크기 때문이다.



〔그림 6〕 F 차분 특성 II : $(a,0)\rightarrow(a\oplus c,0)$



〔그림 7〕 F 차분 특성 III : $(d,a)\rightarrow(a,0)$

〔표 3〕 TYPE 1 및 2의 라운드 별 차분 특성 확률

	TYPE 1	TYPE 2
6-라운드 차분 특성 확률	2^{-110}	2^{-111}
7-라운드 차분 특성 확률	2^{-133}	2^{-133}

다음은 이상에서 살펴 본 두 개의 차분 특성을 정리한 것이다. 6-라운드 차분 특성의 확률은 랜덤한 확률인 2^{-128}보다 좋으므로 차분 공격을 적용할 수 있다. 하지만 TYPE 1 및 2를 1-라운드 확장시킨 확률은 랜덤한 확률보다 낮으므로 기본적인 차분 공격을 적용하기에는 어렵다.

4.2. 새로운 7-라운드 차분 공격

앞서 살펴본 3.2절의 공격 방법을 동일하게 새로운 6-라운드 차분 특성식을 이용하여 적용하면 2^{113}의 데이터 복잡도와 계산 복잡도를 계산하면 $2^{110.19}$의 계산 복잡도로 7-라운드 SEED를 공격할 수 있다.

마찬가지 방법으로 성공 확률을 계산하면 다음과 같다. $\lambda = M1 = 4$이고, 잘못된 키가 카운트 되는 경우는 평균 $\lambda = M2 = 2^{-14}$이 된다. 또한 $k = 4$로 하자.

$$\Pr[X_{M1} \geq 4] = 2^{-32.48}. \quad (3)$$

$$\Pr[X_{M2} \geq 4] = 0.57. \quad (4)$$

옳은 키가 포함될 확률 (4)는 앞서 살펴본 확률 (2)와 같지만, 잘못된 키가 포함될 확률은 앞서 살펴

본 확률보다 현저히 낮아졌다. 따라서 새로운 공격이 기존의 공격보다 효과적으로 적용됨을 알 수 있다.

V. 결 론

본 논문에서의 기존의 6-라운드 차분 특성보다 확률이 좋은 새로운 차분 특성을 제시하였다. 그 결과 기존보다 낮은 복잡도로 7-라운드 SEED를 분석할 수 있음을 보였다. 하지만, 본 논문은 SEED를 분석하는 라운드 수를 늘리지는 못하였다. 이 논문에서 제시한 확률보다 높은 차분 특성식에 대한 연구 및 차분 공격의 2R-attack의 적용 가능성 연구 등을 통해 8-라운드 이상의 SEED의 분석을 수행하는 것이 추후 과제이다.

참고문헌

[1] 김종성, 정기태, 이상진, 홍석희, "새로운 블록 암호 구조에 대한 차분/선형 공격의 안전성 증명," 한국정보보호학회논문지, 17(1), pp. 121-125, 2008년 2월.

[2] 김태현, 김종성, 성재철, 홍석희, "축소된 20-라운드 SMS4에 대한 차분 공격," 한국정보보호학회논문지, 18(4), pp. 37-44, 2008년 8월.

[3] 성재철, 김종성, 이창훈, "가변 라운드 수를 갖는 블록 암호에 대한 차분-연관 암호 공격," 한국정보보호학회논문지, 15(1), pp. 77-86, 2005년 2월.

[4] 성재철, 이상진, 김종수, 임종인, "Skipjack 구조에 대한 DC 및 LC의 안전성," 한국정보보호학회논문지, 10(1), pp. 13-22, 2002년 2월.

[5] 이태건, 고영대, 홍석희, 이상진, "연관키 차분 특성을 이용한 32-라운드 GOST 공격," 한국정보보호학회논문지, 14(3), pp. 75-84, 2004년 6월.

[6] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystem," *Journal of Cryptology*, vol. 4, no. 1, Jan. 1991.

[7] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki and K. Ohta, "A Strategy for Constructing Fast Functions with Practical Security against Differential and Linear Cryptanalysis," SAC 1998, LNCS 1556, pp. 264-270, 1999.

[8] Korea Information Security Agency, "A Design and Analysis of 128-bit Symmetric Block Cipher SEED," 1999. Available at http://www.kisa.or.kr/kisa/seed/jsp/seed_1010.jsp

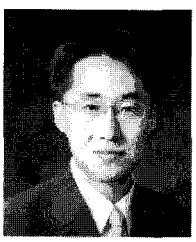
[9] ISO/IEC 18033-3, "Information technology -Security techniques-Encryption algorithms - Part 3: Block Ciphers," 2005.

[10] H. Lipmaa and S. Moriai, "Efficient Algorithms for Computing Differential Properties of Addition," FSE 2001, LNCS 2355, pp. 336-350, 2002.

[11] National Institute of Standards and Technology, "Advanced Encryption Standard," FIPS PUB 197, 2001.

[12] H. Yanami and T. Shimoyama, "Differential Cryptanalysis of a Reduced-Round SEED," SCN 2002, LNCS 2576, pp. 186-198, 2002.

〈著者紹介〉



성 재 철 (Jaechul Sung) 종신회원
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사
2002년 8월~2004년 1월 : 한국정보보호진흥원 선임연구원
2004년 2월~현재 : 서울시립대학교 수학과 전임강사, 조교수, 부교수
〈관심분야〉 암호 알고리즘 설계 및 분석