情報保護學會論文誌
第14券 第3號, 2004. 6

5라운드 KASUMI에 대한 포화공격*

이 제 상[a)†], 이 창 훈[a)], 이 상 진[a)‡], 임 종 인[a)]
고려대학교 정보보호기술연구센터[a)]

Saturation Attacks on the reduced 5-round KASUMI

JeSang Lee[a)†], Changhoon Lee[a)], Sangjin Lee[a)‡], Jongin Lim[a)]
Center for Information of Security of Technologies, Korea University[a)]

요 약

KASUMI는 3GPP에서 사용되는 알고리즘으로, 64비트의 평문을 입력받아 128비트의 키를 사용하여 64비트의 암호문을 출력하는 블록암호이다. 본 논문에서는 10×2^{32} 선택 평문을 이용하여, 공격 복잡도 2^{115}를 갖는 5라운드 포화공격을 소개하고, 중간 일치 공격을 이용하여 공격 복잡도 2^{90}을 갖는 포화공격을 보인다. 더 나아가 *FL6*에 쓰이는 키 아홉 비트가 "111111111"로 고정된 취약 키 클래스에서 7×2^{32}의 선택평문을 이용하여, 공격 복잡도 2^{57}을 갖는 향상된 5라운드 포화공격을 소개한다.

ABSTRACT

KASUMI is a 64-bit iterated block cipher with a 128-bit key size and 8 rounds Feistel structure. In this paper, we describe saturation attacks on the five round KASUMI, which requires 10×2^{32} chosen plaintexts and 2^{115} computational complexity. We also improve this attack using meet-in-the-middle technique. This attack requires 7×2^{32} chosen plaintexts and 2^{90} computational complexity. Futhermore, we attack KASUMI by controlling the value of the fixed part of the key. This attack needs 3×2^{32} chosen plaintexts and 2^{57} computational complexity.

Keywords : *KASUMI, saturation attack, meet-in-the-middle attack, week key*

Ⅰ. 서 론

KASUMI[3]는 IMT2000에서 기밀성 제공을 위해 사용되는 국제 표준 암호 알고리즘이다. 이 암호는 Matsui가 선형공격과 차분공격에 대하여 안전하게 설계한 MISTY[13]를 변형한 것이다. 따라서 KASUMI의 안전성은 MISTY와 마찬가지로 라운드 함수인 *FL* 함수와 *FO* 함수에 의하여 보장된다. KASUMI는 64 비트의 평문을 입력받아 128 비트의 키를 사용하여 64 비트의 암호문을 출력하는 8 라운드 블록 암호이다. 이것은 Feistel 유사구조를 가지고 있으며, 한 라운드는 *FL* 함수와 *FO* 함수로 구성된다.

현재까지, 5 라운드 KASUMI에 대한 포화공격 결과는 전수조사보다 좋지 않다고 알려져 있다[18]. 그러나 본 논문에서는 10×2^{32}의 선택 평문을 이용하여, 전수조사보다 좋은 5 라운드 포화공격을 소개하고, 중간 일치 공격을 이용하여 5 라운드 포화공

접수일 : 2004년 3월 29일 ; 채택일 : 2004년 5월 18일
* 본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자, dogcraft@cist.korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

격을 향상시킬 것이다. 더 나아가, *FL6*에 쓰이는 키가 "111111111"로 고정된 취약 키 클래스하에서 7×2^{32}의 선택평문과 2^{57}의 공격 복잡도를 갖는 향상된 5 라운드 포화공격을 보인다.

본 논문의 구성은 다음과 같다. 2 절에서는 포화공격에 들어가기에 앞서 KASUMI에 대한 간략한 알고리즘 설명과 포화공격에 대한 기본적인 개념 그리고 본 논문에서 사용할 표기법에 대하여 살펴 볼 것이다. 3 절에서는 4 라운드 포화 특성을 구성하고, 기본 5 라운드 포화공격을 보인다. 그리고 이 공격을 향상시키는 방법을 소개할 것이다. 마지막으로 4 절은 본 논문의 결론이다.

II. 준비단계

2.1. KASUMI에 대한 소개

KASUMI는 8 라운드 Feistel 구조의 블록암호로 (그림 1)과 같다. 라운드 함수는 *FL* 함수와 *FO* 함수로 구성되어 있고, 홀수 라운드에서는 *FO* 함수 앞에 *FL* 함수가 위치하며, 짝수 라운드에서는 *FL* 함수 앞에 *FO* 함수가 위치한다. *FL* 함수는 32 비트 키 $KL_i=KL_{i,1}\|KL_{i,2}$에 의하여 결정되는 치환 함수이다. *FO* 함수는 비선형 함수인 세 개의 *FI* 함수로 구성되어 있다. *FI* 함수는 두 개의 S 박스 *S7*, *S9* 로 이루어져 있다. *S7*은 7 비트를 입력받아 7 비트를 출력하고, *S9*는 9 비트를 입력받아 9 비트를 출력하는 비선형함수이다. *FO* 함수와 *FI* 함수에 사용된 키들은 각각 48 비트 $KO_i=KO_{i,1}\|\ KO_{i,2}\|KO_{i,3}$와 48 비트 $KI_i=KI_{i,1}\|KI_{i,2}\|KI_{i,3}$ 이다. 본 논문의 공격에서는 키 스케줄이 사용되지 않으므로 키 생성 과정에 대한 설명은 생략한다.

2.2. 포화공격

포화공격은 주어진 라운드 함수의 일대일 대응 성질을 이용하여 선택된 평문에 대하여 몇 라운드 후의 출력 모양이 포화 집합이 되거나 균일 집합이 되는 성질을 유도하여 올바른 키를 찾아내는 공격방법이다. 포화집합과 균일집합의 정의는 다음과 같다.

- 포화집합(A) : 집합 A를 n 비트로 이루어진 집합이라고 하자. 모든 n 비트 수열들이 집합 A에 정확하게 한 번씩 나타나면, 이때 A를 포화집합이라고 한다.

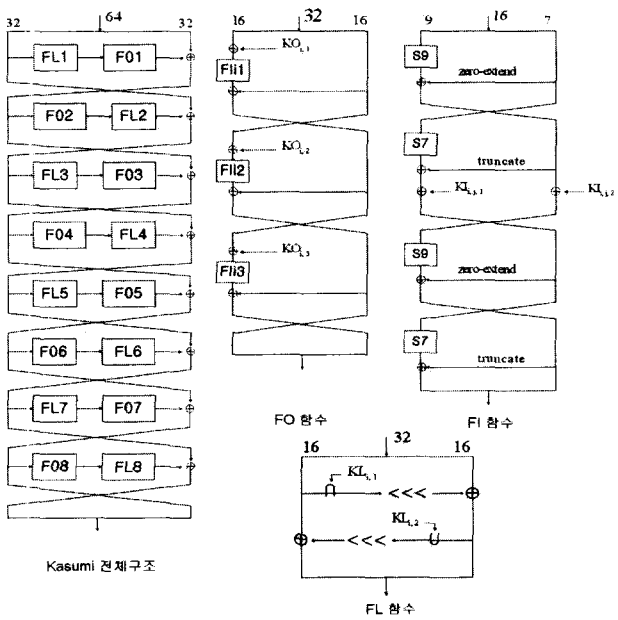


그림 1. KASUMI 알고리즘

• 균일집합(B) : 집합 B를 n 비트 수열들로 구성되어 있다고 하자. 만약 B의 모든 원소들을 XOR한 값이 0이 된다면, 즉

$$\bigoplus_{x_i \in B} x_i = 0$$

하면, 이 때 집합 B를 균일집합이라고 한다.

어떤 집합 A가 포화집합이면 A는 균일집합이 된다는 사실은 정의로부터 쉽게 알 수 있다. 또한 포화집합과 균일집합에 대한 XOR 연산의 특성은 〔표 1〕과 같다[17].

표 1. XOR 연산의 특성의 특성

XOR (⊕)	포화집합 (A)	상수 (C)	균일집합 (B)
포화집합 (A)	균일집합 (B)	포화집합 (A)	균일집합 (B)
상수 (C)	포화집합 (A)	상수 (C)	균일집합 (B)
균일집합 (B)	균일집합 (B)	균일집합 (B)	균일집합 (B)

2.3. 표기법

본 소절에서는 본 논문에서 사용될 표기법에 대하여 소개할 것이다.

i = 짝수 일 때 $X_i \in GF(2)^7$ 이고, i = 홀수 일 때 $X_i \in GF(2)^9$ 라 하면,

• 평문 :

$$\begin{aligned} P &= (PL \parallel PR) \\ &= (P_7, \cdots, P_4 \parallel P_3, \cdots, P_0) \end{aligned}$$

• 각 i라운드의 입력 값 :

$$\begin{aligned} Z^i &= (Z^i_L \parallel Z^i_R) \\ &= (Z^i_7, \cdots, Z^i_4 \parallel Z^i_3, \cdots, Z^i_0) \end{aligned}$$

• 5라운드로 축소된 KASUMI의 암호문 :

$$\begin{aligned} C &= (CL \parallel CR) \\ &= (C_7, \cdots, C_4 \parallel C_3, \cdots, C_0) \end{aligned}$$

위의 표기법에 의하여 $(P_7, \cdots, P_4 \parallel P_3, \cdots, P_0) = (Z^1_7, \cdots, Z^1_4 \parallel Z^1_3, \cdots, Z^1_0)$ 라는 사실을 쉽게 도출할 수 있다. 더 나아가, "$\parallel$"은 연접을 의미하며, "$\wedge$"은 비트별 AND 연산을 의미한다. 마지막으로 "T"는 최상위 2 비트 버림을 의미한다.

III. 포화공격

3.1. KASUMI의 4 라운드 포화 특성

이 소절에서는 5 라운드 포화공격에 사용할 4 라운드 포화 특성을 구성할 것이다. 위에서 언급한 포화 성질을 이용하면, 다음과 같은 포화 특성을 간단하게 이끌어 낼 수 있다.

먼저 평문 집합으로 $P = (C, A)$을 선택한다. 여기서 C 는 고정된 임의의 32 비트 상수 값이고, A는 32 비트의 포화집합이다. 키가 고정되었을 때, FL 함수와 FO 함수가 일대일 대응 성질을 만족하므로, (그림 2)와 같이, 선택 평문 집합 $P=(C, A)$에 대하여 다섯 번째 라운드 입력 부분에서 $Z^5 = (?, B)$ 특성을 얻을 수 있다. 여기서 B 는 균일 집합을 말한다. 즉, 5 라운드 입력 값 Z^5_R 에서 균일 성질

$$\bigoplus_{w_i \in Z^5_R} w_i = 0$$

을 만족한다.

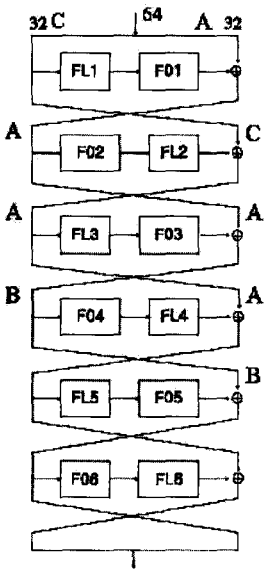


그림 2. KASUMI 포화특성

3.2. KASUMI 5 라운드 포화 공격

이 소절에서는 앞 소절에서 구성한 4 라운드 포화 특성를 이용하여 5 라운드 포화공격을 소개한다.

평문집합 $P = (C, A)$에 대응하는 암호문 집합 $C = (CL \| CR)$의 오른쪽 출력 CR 값들에 대하여 다섯 번째 라운드를 복호화한다고 가정하자. $FL5(CR_i, KL_{5,1}, KL_{5,2}) = (X_{Li} \| X_{Ri})$이라 할 때, $FL5$ 함수 키 $KL_{5,1}$과 $KL_{5,2}$를 추측하면 X_{Li}과 X_{Ri}의 값을 알 수 있다. X_{Li}을 $FO5$의 첫 번째 라운드 키 $KO_{5,1}$, $KI_{5,1,2}$을 추측하여 복호화하고, X_{Ri}을 $FO5$의 두 번째 라운드 키 $KO_{5,2}$, $KI_{5,2,2}$를 추측하여 복호화한 뒤, 복호화된 집합과 그 값에 대응되는 왼쪽 출력 암호문 집합을 XOR 하면, 그 값에서 균일 성질이 나타남을 알 수 있다. 앞 소절에 제시한 포화 특성에 의하여 균일 성질이 나타나는 키는 옳은 키로 간주하고, 그렇지 않은 키는 틀린 키로 버린다.

여기서 $KI_{5,1,1}$ 과 $KI_{5,2,1}$ 을 추측하지 않는 이유는 공격에서 이끌어내고자 하는 균일 성질에 아무런 영향을 주지 않기 때문이다.

즉 , $FL5(CR, KL_{5,1}, KL_{5,2}) = (C_3', C_2', C_1', C_0')$이고, $a_i \in C_3', b_i \in C_2', c_i \in C_1', d_i \in C_0'$ 일 때,

$$\bigoplus_{w_i \in ((Z_3^5 \wedge 3) \| Z_2^5)} w_i = \bigoplus_i \left\{ \begin{array}{l} (00 \| (T(S_9(a_i) \oplus (00 \| b_i)) \oplus S_7(b_i) \oplus KI_{5,1,1})) \\ \oplus S_9(S_9(a_i) \oplus (00 \| b_i) \oplus KI_{5,1,2}) \oplus ((c_i \wedge 3) \| d_i) \\ \oplus (00 \| (T(S_9(c_i) \oplus (00 \| d_i)) \oplus S_7(d_i) \oplus KI_{5,2,1})) \\ \oplus S_9(S_9(c_i) \oplus (00 \| d_i) \oplus KI_{5,2,2}) \oplus ((C_7 \wedge 3) \| C_6) \end{array} \right\} = 0 \quad (1)$$

이다. 그리고 XOR 연산은 선형이므로

$$\bigoplus_{w_i \in ((Z_3^5 \wedge 3) \| Z_2^5)} w_i = \bigoplus_i \left\{ \begin{array}{l} (00 \| (T(S_9(a_i) \oplus (00 \| b_i)) \oplus S_7(b_i))) \\ \oplus S_9(S_9(a_i) \oplus (00 \| b_i) \oplus KI_{5,1,2}) \oplus ((c_i \wedge 3) \| d_i) \\ \oplus (00 \| (T(S_9(c_i) \oplus (00 \| d_i)) \oplus S_7(d_i))) \\ \oplus S_9(S_9(c_i) \oplus (00 \| d_i) \oplus KI_{5,2,2}) \oplus ((C_7 \wedge 3) \| C_6) \\ \oplus KI_{5,1,1} \oplus KI_{5,2,1} \end{array} \right\} = 0 \quad (2)$$

이 된다. $KI_{5,1,1}$와 $KI_{5,2,1}$는 공격에서 추측한 값이므로,

$$\bigoplus_{w_i \in ((Z_3^5 \wedge 3) \| Z_2^5)} w_i = \bigoplus_i \left\{ \begin{array}{l} (00 \| (T(S_9(a_i) \oplus (00 \| b_i)) \oplus S_7(b_i))) \\ \oplus S_9(S_9(a_i) \oplus (00 \| b_i) \oplus KI_{5,1,2}) \oplus ((c_i \wedge 3) \| d_i) \\ \oplus (00 \| (T(S_9(c_i) \oplus (00 \| d_i)) \oplus S_7(d_i))) \\ \oplus S_9(S_9(c_i) \oplus (00 \| d_i) \oplus KI_{5,2,2}) \oplus ((C_7 \wedge 3) \| C_6) \end{array} \right\} = 0 \quad (3)$$

라 할 수 있다. 따라서, 키 $KI_{5,1,1}$과 $KI_{5,2,1}$가 $(Z_3^5 \wedge 3) \| Z_2^5$의 균일성질에 영향을 주지 않으므로, $KI_{5,1,1}$와 $KI_{5,2,1}$를 추측하지 않아도 Z_2^5의 균일 성질을 만족하는지를 체크할 수 있다.

공격 시나리오를 정리하자면, 5 라운드 포화공격을 통하여 다섯 번째 라운드의 82 비트 부분키 $K = \{KO_{5,1}, KO_{5,2}, KI_{5,1,2}, KI_{5,2,2}, KL_{5,1}, KL_{5,2}\}$를 추측하여 암호문을 (그림 3)과 같이 복호화해서, 5 라운드의 오른쪽 입력 상위 8 번째 비트부터 16 번째 비트까지 균일성질

$$\bigoplus_{w_i \in ((Z_3^5 \wedge 3) \| Z_2^5)} w_i = 0$$

을 만족하면 옳은 키로 간주하고, 만족하지 않으면 틀린 키로 간주하고 버린다.

선택 평문 집합 $P = (C, A)$ 에 대하여, 올바른 키가 아니면서 82 비트 부분키가 수식 (3)을 만족할 확률은 2^{-9}이다. 따라서 부분키 공간의 크기가 2^{82}이라고 할 때, 확률적으로 올바른 키를 찾아내기 위해서는 적어도 10개의 선택 평문 집합이 필요하다.

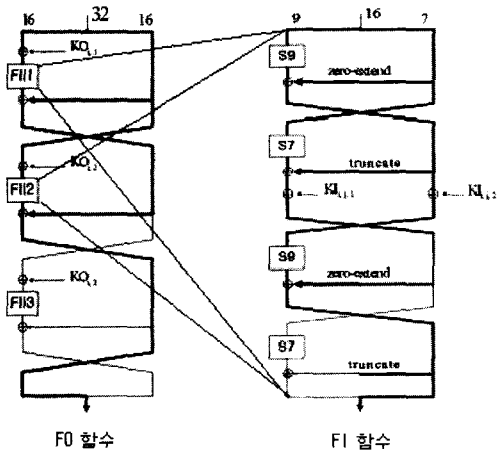


그림 3. 5 라운드 FO 함수 키 추출 경로

따라서 5 라운드 포화 공격 복잡도는 선택 평문 집합 10개에 대하여 82 비트의 부분키를 전수 조사하여 찾아내므로 $\frac{1}{5} \times 10 \times 2^{32} \times 2^{82} = 2^{115}$라 할 수 있다.

3.3 중간 일치 공격을 이용한 KASUMI 5 라운드 포화 공격

이 소절에서는 앞 소절에서 제시한 5 라운드 포화 공격을 중간 일치 공격을 이용하여 향상시킬 것이다. 앞 절에서 제시한 포화 공격은 $FL5$ 함수와 $FO5$ 함수를 복호화하여, 왼쪽 출력 하위 아홉 비트의 균일 성질을 이용한 공격이었다. 이 절에서는 $FO5$ 함수에 적용되는 키 $KO_{5,1}$, $KI_{5,1,2}$와 $KO_{5,2}$, $KI_{5,2,2}$을 독립적으로 추측하여 공격 복잡도를 낮출 것이다.

$FL5(CR_i, KL_{5,1}, KL_{5,2}) = (X_{Li} \| X_{Ri})$ 이라 할 때, X_{Li}을 $FO5$의 첫 번째 라운드 키 $KO_{5,1}$, $KI_{5,1,2}$을 추측하여 복호화하고, X_{Ri}을 $FO5$의 두 번째 라운드 키 $KO_{5,2}$, $KI_{5,2,2}$를 추측하여 복호화한 뒤, 복호화 된 집합과 그 값에 대응되는 왼쪽 출력 암호문 집합을 XOR 하면, 그 값에서 균일 성질이 나타나는가를 체크하였다.

키 $KO_{5,1}$, $KI_{5,1,2}$이 쓰이는 부분의 함수와 $KO_{5,2}$, $KI_{5,2,2}$가 쓰이는 부분의 함수를 각 각 f와 g라 하고, $KI_{5,1,1}$, $KI_{5,2,1}$ 그리고 암호문 $(C_7 \wedge 3) \| C_6$ 에 의하여 결정되는 값을 C' 라 하면, $f_{KO_{5,1}, KI_{5,1,2}}(X_L) \oplus g_{KO_{5,2}, KI_{5,2,2}}(X_R) \oplus C'$ 을 왼쪽 출력 하위 아홉 비트에 대하여 조사할 수 있다. 위 수식을 통하여

$$\bigoplus_i \{f_{KO_{5,1}, KI_{5,1,2}}(X_{Li}) \oplus g_{KO_{5,2}, KI_{5,2,2}}(X_{Ri})\} = \bigoplus_i C'_i$$

을 이끌어 낼 수 있다. 위 수식을 이용하여 중간일치 공격을 이용한 포화 공격을 수행할 수 있다. KASUMI의 중간 일치 공격을 이용한 포화공격은 다음과 같다.

- **1 단계** : 평문 집합에 대응하는 암호문 집합 CR을 $KL_{5,1}$, $KL_{5,2}$을 추측하여 복호화 한다.
- **2 단계** : 1 단계에서 복호화한 집합 CR'에 대하여, 5 라운드의 부분키 $KO_{5,1}$, $KL_{5,1,2}$을 추측하여 CR'을 복호화하여,

$$\bigoplus_i f_{KO_{5,1}, KI_{5,1,2}}(CR'_i)$$

을 구한 뒤 테이블 1 에 각각의 값을 저장한다.
- **3 단계** : 1 단계에서 복호화한 집합 CR'에 대하여, 5 라운드의 부분키 $KO_{5,2}$, $KL_{5,2,2}$을 추측하여 CR'을 복호화하여,

$$\bigoplus_i g_{KO_{5,2}, KI_{5,2,2}}(CR'_i)$$

을 구한 뒤 테이블 2 에 각 각의 값을 저장한다.
- **4 단계** : 위에서 저장한 테이블 1과 2의 값을 XOR 한 값이 평문 집합에 대응하는 암호문 집합을 XOR한 값과 일치하는지 조사한다. 일치하면 옳은 키로 간주하고, 그렇지 않은 키는 버린다.
- **5 단계** : 위의 과정을 유일한 키 한 개가 남을 때까지 다양한 평문 집합에 대하여 반복한다.

선택 평문 집합 $P=(C, A)$에 대하여 82비트 옳지 않은 키가 위의 성질을 만족할 확률은 아홉 비트의 균일 성질을 이용하므로 2^{-9}이다. 여기에서 $KO_{5,1}$, $KL_{5,1,2}$ 와 $KO_{5,2}$, $KL_{5,2,2}$는 단계 1과 단계 2에서 독립적으로 추측되므로 57 비트의 키를 2개 독립적으로 추측하는 것과 같다. 따라서 부분키 공간의 크기가 2^{57}이라고 할 때, 확률적으로 옳은 키를 찾아내기 위해서는 적어도 선택 평문 집합 7개가 필요하다. 따라서 5 라운드 KASUMI에 대한 포화 공격 복잡도는 약 $2 \times \frac{1}{5} \times 7 \times 2^{32} \times 2^{57} \approx 2^{90}$ 라 할 수 있다.

본 공격은 앞 소절의 공격과 다르게 균일값을 저장하는 테이블이 이용되므로 메모리가 요구된다. $FL5$ 함수의 키 $KL_{5,1}$, $KL_{5,2}$에 대하여 $FO5$ 함수의 키 $KO_{5,1}$, $KL_{5,1,2}$와 $KO_{5,2}$, $KL_{5,2,2}$을 독립적으로 추측하여 균일값을 두 개의 테이블에 각각 저장하므로, 공격을 성공시키기 위하여 $2 \times 2^{32} \times 2^{25} = 2^{58}$의 메모리가 필요하다.

3.4 취약 키 클래스 KASUMI 5 라운드 포화 공격

이 소절에서는 앞 절에서 구성한 5 라운드 포화 공격을 $FL6$ 함수의 키 $KL_{6,2,2}$의 9 비트가

"111111111"로 고정된 취약 키 클래스에 대하여 향상시킬 것이다. 앞 소절에서 제시한 공격을 더욱 더 향상시키기 위하여 1~5 라운드 포화공격이 아닌, 2~6 라운드 포화 공격을 구성할 것이다.

(그림 2)에 나타난 포화특성을 2 라운드부터 구성하면, 즉 2 라운드 입력 값을 $Z^2=(C,A)$ 로 선택하면 4 라운드 포화특성 $Z^6=(?,B)$를 얻을 수 있다. 이 4 라운드 포화특성을 이용하여 5 라운드(2 ~ 6라운드) 포화 공격을 시도한다.

이 공격에서는 $FL6$ 함수를 제외한 $FO6$에 쓰이는 부분키만을 찾을 것이다. 6 라운드의 부분키 후보 $K=\{KO_{6,1}, KO_{6,2}, KI_{6,1,2}, KI_{6,2,2}\}$를 이용하여 중간 일치 공격을 이용한 5 라운드 기본 공격과 같은 방법으로 암호문을 복호화하면, $CR=(X_L||X_R)$이라 할 때, $f_{KO_{6,1},KI_{6,1,2}}(X_L)$을 $\oplus g_{KO_{6,2},KI_{6,2,2}}(X_R)$ 구할 수 있다.

(그림 4)를 보면 알 수 있듯이, $f_{KO_{6,1},KI_{6,1,2}}(X_L)$ $\oplus g_{KO_{6,2},KI_{6,2,2}}(X_R)$이 XOR되는 $KL_{6,2,2}$의 9비트 키를 "111111111"로 고정시키면,

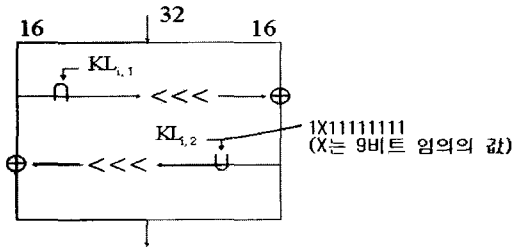


그림 4. FL함수 취약키 특성

$$\bigoplus_i \{f_{KO_{5,1},KI_{5,1,2}}(X_{Li}) \oplus g_{KO_{5,2},KI_{5,2,2}}(X_{Ri}) \oplus 111111111\} = \bigoplus_i C'_i$$

"111111111"은 고정된 상수 값이므로,

$$\bigoplus_i \{f_{KO_{5,1},KI_{5,1,2}}(X_{Li}) \oplus g_{KO_{5,2},KI_{5,2,2}}(X_{Ri})\} = \bigoplus_i C'_i$$

이다. FL 함수의 입력 값

$$\bigoplus_i \{f_{KO_{5,1},KI_{5,1,2}}(X_{Li}) \oplus g_{KO_{5,2},KI_{5,2,2}}(X_{Ri})\}$$

이 그대로 유지됨을 알 수 있다. 따라서 앞 절에서 제시한 중간 일치 공격을 그대로 적용할 수 있다.

선택 평문 집합에 대하여, 옳은 키가 아니면서 50 비트 부분 키가 위의 성질을 만족할 확률은 2^{-9}이다. 여기에서 $KO_{6,1}$, $KI_{6,1,2}$와 $KO_{6,2}$, $KI_{6,2,2}$는 독립적으로 추측되므로 25 비트의 키를 2개 독립적으로 추측하는 것과 같다. 부분키 공간의 크기가 2×2^{25}이므로 확률적으로 옳은 키를 찾아내기 위해서는 적어도 3 개의 선택 평문 집합이 필요하다.

이 절에서 5 라운드 포화 공격 복잡도는 2^{32}의 평문 집합 7 개에 대하여 50 비트의 부분키를 전수조사하여 찾아내므로, $2\times\frac{1}{5}\times3\times2^{32}\times2^{25}\approx2^{57}$라 할 수 있다.

앞 소절과 마찬가지로 균일값을 저장하기 위하여 테이블이 사용되므로 다음과 같은 메모리가 요구된다. $FO6$ 함수의 키 $KO_{6,1}$, $KI_{6,1,2}$와 $KO_{6,2}$, $KI_{6,2,2}$을 독립적으로 추측하여 균일 값을 두 개의 테이블에 각각 저장하므로, 공격을 성공시키기 위하여 $2\times2^{25}=2^{26}$의 메모리가 필요하다.

IV. 결 론

본 논문의 5라운드 KASUMI에 대한 포화공격 결과를 요약하면 [표 3]과 같다. 지금까지 5라운드 KASUMI 포화 공격은 전수조사보다 좋지 않다고 알려져 있었다. 그러나 본 논문에서는 전수조사보다

표 2. 기존 KASUMI 공격 결과

공격 방법	라운드 수	선택 평문수	공격 복잡도
연관키 공격[15]	6	2^{48}	2^{112}
불능 차분 공격[10]	6 (2-7)	2^{50}	2^{100}

표 3. 5 라운드 KASUMI 포화공격 결과

공격 방법	선택 평문수	공간 복잡도	공격 복잡도
기본공격	10×2^{32}	·	2^{115}
중간일치 공격	7×2^{32}	2^{58}	2^{90}
취약 키	7×2^{32}	2^{26}	2^{57}

나은 포화공격을 성공시켰을 뿐만 아니라, 기본 포화공격을 중간일치 공격을 이용하여 공격 복잡도를 향상시켰다. 더 나아가 9비트 키가 "111111111"로 고정된 취약 키 클래스 하에서 포화공격을 더욱 향상시킬 수 있다.

참 고 문 헌

[1] P. Barreto, V. Rijmen, J. Nakahara Jr., B. Preneel, J. Vandewalle, and H. Y. Kim. "Improved SQUARE attacks against reduced-round HIEROCRYPT", *FSE 2001*, LNCS 2355, Springer-Verlag 2002, pp. 165-173.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", In Journal of cryptology, vol 4, no 1, 1991, pp. 3-72.

[3] ETSI/SAGE. "Specification of the 3GPP Confidentiality and Integrity Algorithms - Document 2: KASUMI Specification", Version 1.0.3G TS 35.202. December 23, 1999.http://www.3gpp.org/TB/Other/algorithms.htm

[4] Y. He, S. Qing, "Square Attack on Reduced Camellia Cipher", *ICICS 2001*, LNCS 2229, Springer-Verlag 2002, pp. 89-99.

[5] Hidema TANAKA, Chikashi ISHII, Toshimobu KANEKO. "On the strength of KASUMI without FL functions against Higher Order Differential Attac", *ICISC 2000*, LNCS 2015, Springer-Verlag 2001, pp. 14-21.

[6] Y. Hu, Y. Zhang, and G. Xiao, "Integral cryptanalysis of SAFER+", *IEE*, vol 35, no 17, 19. Aug. 1999, pp. 1458-1459.

[7] L.R. Knudsen. "Truncated and higher order differentials", *FSE 1994*, LNCS 1008, Springer-Verlag 1995, pp 196-211.

[8] L.R. Knudsen, D. Wagner, "Integral Cryptanalysis", *FSE 2002*, LNCS 2365, Springer Verlag 2002, pp. 112- 127.

[9] Ulrich Kuhn, "Crypanalysis of Reduced-Round MISTY", *EUROCRYPT 2002*, LNCS 2045, Springer-Verlag 2001, pp. 325-339.

[10] Ulrich Kuhn, "Improved Cryptanalysis of MISTY", *FSE 2002*, LNCS 2365, Springer-Verlag 2002, pp. 61-75.

[11] X. Lai, "Higher Order Derivations and Differential Cryptanalysis", Communications and Cryptography : Two Sides of one Tapestry, Kluwer Academic Publishers, 1994, pp. 227-233.

[12] S. Lucks, "The Saturation Attack - a Bait for Twofish", *FSE 2001*, LNCS 2355, Springer-Verlag 2002, pp. 1-15.

[13] M. Matsui. "New block encryption algorithm MISTY", In E. Biham, editor, *FSE 1997*, LNCS 1267, Springer- Verlag 1997, pp. 54-68.

[14] Mark Blunden, Adrian Escott, "Related Key Attacks on Reduced Round KASUMI", *FSE 2001*, LNCS 2355, Springer-Verlag 2002, pp. 277-285.

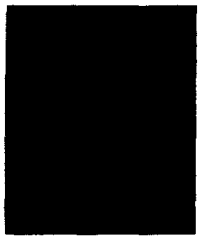
[15] K. Nyberg. "Generalized Feistel networks". Advances in Cryptology - *ASIACRYPT'96*, LNCS 1163, Springer-Verlag 1996, pp. 91-104.

[16] K. Sakurai and Y. Zheng, "On Non-Pseudorandomness from block Ciphers with Provable Immunity against Cryptanalysis", *IEICE 1997*, vol E80-A, no 1, 1997, pp. 19-24.

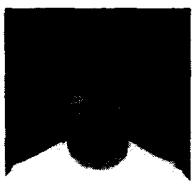
[17] Yongjin Yeom, Sangwoo Park, Iljun Kim, "On the Security of CAMELLIA against the Square Attack", *FSE 2002*, LNCS 2365, Springer-Verlag 2002, pp. 89-99.

[18] Vebjørn Moen, "Integral Cryptanalysis of Block Ciphers", Master, Bergen University, May 6. 2002.

〈著者紹介〉

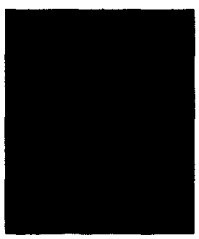


이 제 상 (Je-sang Lee)
2003년 2월 : 고려대학교 수학과 학사
2003년 3월~현재 : 고려대학교 정보보호대학원 석사과정
〈관심분야〉 대칭키 암호의 분석 및 설계, 정보은닉이론, DRM



이 창 훈 (Changhoon Lee)
2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2003년 3월~현재 : 고려대학교 정보보호대학원 박사과정
〈관심분야〉 대칭키 암호의 분석 및 설계

이 상 진 (Samgjin Lee) 정회원
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수,
2001년 9월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식



임 종 인 (Jong-in Lim) 정회원
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1986년 9월~2001년 1월 : 고려대학교 자연과학대학 정교수
2001년 2월~현재 : 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 암호 이론, 암호 정책, PET