블록암호 KASUMI에 대한 포화공격

이제상* 이태건* 이창훈* 이원일* 홍석희* 이상진*

*고려대학교 정보보호대학원

Square Attacks of Reduce-Round in KASUMI

Jesang Lee*, Taekeon Lee*, Changhoon Lee*, Wonil Lee*, Seokhie Hong*, Sangjin Lee*

*Graduate School of Information Security, Korea University

요 약

본 논문에서는 5-라운드 KASUMI의 포화공격에 대하여 다룰 것이다. KASUMI는 3GPP에서 사용되는 알고리즘으로, 64비트의 평문을 입력받아 128비트의 키를 사용하여 64비트의 암호문을 출력하는 블록암호이다. 본 논문에서는 10×2^{32}의 선택 평문을 이용하여, 공격 복잡도 2^{115}를 갖는 5라운드 포화공격(Square Attack)을 소개할 것이다. 또한, 이 공격은 함수의 키를 9비트 고정함으로서 향상시킬 수 있다. 이러한 경우, 7×2^{32}의 선택평문을 이용하여, 공격 복잡도 2^{83}을 갖는 5라운드 포화공격을 성공시킬 수 있다.

I. 서론

KASUMI[1]는 3세대 이동 통신 IMT2000에서 기밀성을 위해 사용되는 국제 표준 암호 알고리즘이다. 이 암호는 Matsui가 선형공격과 차분공격에 대하여 안전하게 제안한 MISTY[2]를 변형한 것이다. MISTY와 마찬가지로 KASUMI의 안전성은 라운드함수인 *FL*함수와 *FO*함수에 의하여 보장된다. KASUMI는 64비트의 평문을 입력받아 128 비트의 키를 사용하여 64비트의 암호문을 출력하는 알고리즘으로 DES와 같은 feistel구조를 가지며, 라운드 함수 *FL*과 *FO*로 구성된 8 라운드 블록암호이다.

현재까지, 5라운드 KASUMI 포화공격의 공격 결과는 전수조사보다 좋지 않다고 알려져 있다. 따라서 본 논문에서는 10×2^{32}의 선택 평문을 이용하여, 전수조사보다 좋은 5라운드 포화공격을 소개할 것이다. 또한, 7×2^{32}의 선택평문을 이용하여, 공격 복잡도 2^{83}을 갖는 향상된 5 라운드 포화공격을 보이겠다.

본 논문은 다음과 같이 구성되어 있다. 2절은 KASUMI의 알고리즘을 간단히 소개하고 포화공격에 대한 개념을 설명할 것이다. 3절에서는 4라운드 distinguisher를 구성하여 5라운드 포화공격을 보일 것이다. 마지막으로 4절은 본 논문의 결론을 도출할 이다.

II. 준비단계

1. KASUMI

KASUMI는 8라운드 feistel구조의 블록암호이다. 라운드함수는 *FL* 함수와 *FO* 함수로 구성되어있다. 홀수 라운드에서는 *FO* 함수 앞에 *FL* 함수가 위치하고, 짝수라운드에서는 *FL* 함수 앞에 *FO* 함수가 위치한다. *FL* 함수는 그림 4 와 같이 구성되어 있으며, 키 32 비트 ($KL_i = KL_{i,1} \| KL_{i,2}$)가 고정되면 일대 일 대응 함수이다. *FO*함수는 그림 2 와 같으며, 각 라운드의 비선형인 부분으로써 세 개의 *FI* 함수로 구성되어 있고, *FI* 함수 그림 3과 같으며, *FI* 함수 안에는 각각 두개씩의 *S7*, *S9*인 S-box로 이루어져 있다. *S7*은 7비트를 입력받아 7비트를 출력하는 함수이고 *S9*는 9비트를 입력받아 9비트를 출

력하는 비선형함수이다. *FO*함수와 *FI*함수에 사용된 키들은 각각 48비트 $KO_i = KO_{i,1} \| KO_{i,2} \| KO_{i,3}$와 48비트 $KI_i = KI_{i,1} \| KI_{i,2} \| KI_{i,3}$이다. 본 논문의 공격에서는 키 스케줄이 사용되지 않으므로 키 생성과정에 대하여 자세한 설명은 생략한다.

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 찾아낸다. 포화집합과 균일집합의 정의는 다음과 같다:

• 포화집합(A) : 집합 *M*을 모든 *n*비트 수열들의 집합의 원소들로 구성되어 있다고 하자. 모든 *n*비트 수열들이 *M*에 정확하게 한번씩 나타난다면 이때 *M*을 포화집합 이라고 한다.

• 균일집합(B) : 집합 *N*을 *n*비트 수열들의 집합의 원소들로 구성되어 있다고 하자. 만일 *N*의 모든 원소들을 XOR한 값이 0이 된다면 ($\oplus x_i = 0$, $x_i \in N$) 이 때 *N*을 균일집합이라고 한다. 어떤 집합 *M*이 포화집합이면 *M*은 균일집합이 된다는 사실을 쉽게 알 수 있다.

포화집합과 균일집합에 대한 XOR연산의 특성은 다음과 같다.

표 1 : XOR연산의 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)

3. 표기법

KASUMI 의 구조는 그림 1과 같으며, 평문은 다음과 같이 표현된다.

• $P = (PL \| PR)$

$= (X_7, \cdots, X_4 \| X_3, \cdots, X_0)$

$X_i \in GF(2)^7$: $i =$ 짝수

$X_i \in GF(2)^9$: $i =$ 홀수

그리고, 각 라운드의 입력 값은 다음과 같이 표현된다.

• $Z^i = (Z^i_L \| Z^i_R)$

$= (Z^i_7 \cdots, Z^i_4 \| Z^i_3 \cdots, Z^i_0)$

$Z_i \in GF(2)^7$: $i =$ 짝수

$Z_i \in GF(2)^9$: $i =$ 홀수

여기서 *i*는 라운드를 말한다.

따라서, $(X_7, \cdots, X_4 \| X_3, \cdots, X_0)$

$= (Z^1_7 \cdots, Z^1_4 \| Z^1_3 \cdots, Z^1_0)$

또한, 5라운드로 축소된 KASUMI의 암호문은 다음과 같이 표현된다.

• $C = (CL \| CR)$

$= (Y_7, \cdots, Y_4 \| Y_3, \cdots, Y_0)$

$Y_i \in GF(2)^7$: $i =$ 짝수

$Y_i \in GF(2)^9$: $i =$ 홀수

• || : 연접

• ∧ : 비트별 AND 연산

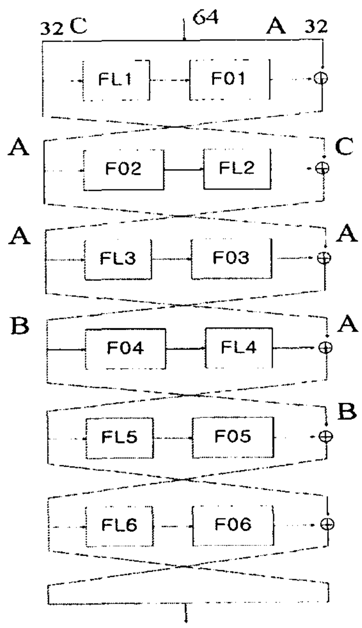

그림 1 KASUMI

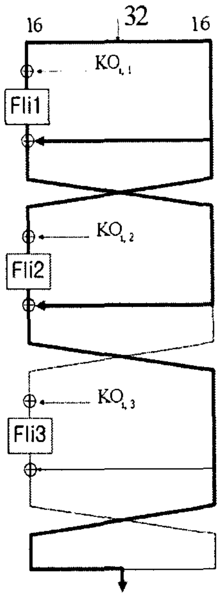

그림 2 *FO*함수

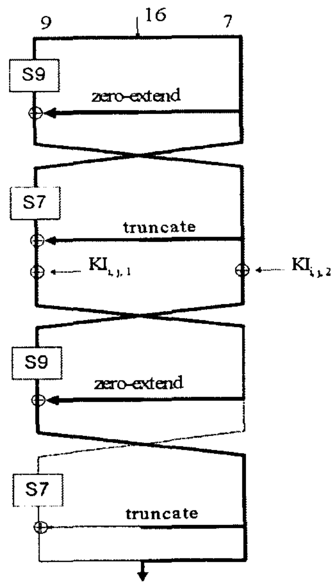

그림 3 *FI*함수

III. 포화공격

1. KASUMI의 4라운드 포화 특성

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

우리는 먼저 평문 집합으로 $P=(C,A)$ 을 선택한다. 여기서 C는 고정된 임의의 32비트의 상수 값이고, A는 32비트의 포화집합이다.

그러면, 그림1 에서와 같이, 선택 평문 집합 $P=(C,A)$에 대하여 다섯 번째 라운드 오른쪽 입력에서 $Z^5=(?,B)$특성을 얻을 수 있다. 즉, 5 라운드 입력 값 Z^5_R에서 균일 성질

($\bigoplus_{w_i \in ((Z^5_3 \wedge 3) \| Z^5_2)} w_i = 0$) 이 나타나는 것을 알 수 있다.

2. KASUMI 5라운드 포화 공격

이 절에서는 앞 절에서 구성한 4라운드 distinguisher를 이용하여 5라운드 포화 공격을 한다. 그러면, 5번째 라운드의 82비트 부분키를 다음과 같이 찾아 낼 수 있다.

5라운드의 부분키 후보

$K=\{KO_{5,1}, KO_{5,2}, KI_{5,1,2}, KI_{5,2,2}, KL_{5,1}, KL_{5,2}\}$

82 비트를 추측하여 암호문을 그림 3과 같이 복호화 하면, 4라운드의 오른쪽 출력 상위 8번째 비트부터 16번째 비트까지 균일성질

($\bigoplus_{w_i \in ((Z^5_3 \wedge 3) \| Z^5_2)} w_i = 0$)을 이끌어 낼 수 있다. 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,

$FL5(CR, KL_{5,1}, KL_{5,2}) = (C_3', C_2', C_1', C_0')$ 일 때,

$$\begin{aligned}
&\bigoplus_{w_i \in ((Z^5_3 \wedge 3) \| Z^5_2)} w_i = \\
&\bigoplus \left(\begin{array}{l}
(00 \| (T(S_9(a_i') \oplus (00 \| b_j')) \oplus S_7(b_j') \oplus KI_{5,1,1})) \\
\oplus S_9(S_9(a_i') \oplus (00 \| b_j') \oplus KI_{5,1,2}) \oplus ((C_1 \wedge 3) \| C_0) \\
\oplus (00 \| (T(S_9(c_l') \oplus (00 \| d_m')) \oplus S_7(d_m') \oplus KI_{5,2,1})) \\
\oplus S_9(S_9(c_l') \oplus (00 \| d_m') \oplus KI_{5,2,2}) \oplus ((Y_7 \wedge 3) \| Y_6)
\end{array} \right) \\
&= 0 \qquad (a_i \in C_3', b_j \in C_2', c_l \in C_1', d_m \in C_0')
\end{aligned} \tag{1}$$

이다. 그리고 XOR 연산은 선형이므로

$$
\bigoplus_{w_i\in((Z_3^5\wedge 3)\|Z_2^5)} w_i =
\bigoplus \left(\begin{array}{l}
(00\|(T(S_9(a_i')\oplus(00\|b_j'))\oplus S_7(b_j'))) \\
\oplus S_9(S_9(a_i')\oplus(00\|b_j')\oplus KI_{5,1,2})\oplus((C_1\wedge 3)\|C_0) \\
\oplus(00\|(T(S_9(c_l')\oplus(00\|d_m'))\oplus S_7(d_m'))) \\
\oplus S_9(S_9(c_l')\oplus(00\|d_m')\oplus KI_{5,2,2})\oplus((Y_7\wedge 3)\|Y_6) \\
\oplus KI_{5,1,1}\oplus KI_{5,2,1}
\end{array} \right)
$$
$$
=0 \qquad (a_i\in C_3', b_j\in C_2', c_l\in C_1', d_m\in C_0') \tag{2}
$$

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

$$
\bigoplus_{w_i\in((Z_3^5\wedge 3)\|Z_2^5)} w_i =
\bigoplus \left(\begin{array}{l}
(00\|(T(S_9(a_i')\oplus(00\|b_j'))\oplus S_7(b_j'))) \\
\oplus S_9(S_9(a_i')\oplus(00\|b_j')\oplus KI_{5,1,2})\oplus((C_1\wedge 3)\|C_0) \\
\oplus(00\|(T(S_9(c_l')\oplus(00\|d_m'))\oplus S_7(d_m'))) \\
\oplus S_9(S_9(c_l')\oplus(00\|d_m')\oplus KI_{5,2,2})\oplus((Y_7\wedge 3)\|Y_6)
\end{array} \right)
$$
$$
=0 \qquad (a_i\in C_3', b_j\in C_2', c_l\in C_1', d_m\in C_0') \tag{3}
$$

라 할 수 있다. 따라서, 키 정보가 Z_2^5의 균일성질에 영향을 주지 않으므로, 우리는 $KI_{5,1,1}$와 $KI_{5,2,1}$를 추측하지 않아도 Z_2^5의 균일 성질을 알 수 있다.

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

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

3. 향상된 KASUMI 5-라운드 포화 공격

이 절에서는 앞 절에서 구성한 5 라운드 포화 공격을 향상시킬 것이다. 본 공격을 향상시키기 위하여 1~5 라운드 포화공격이 아닌, 2~6 라운드 포화 공격을 구성할 것이다. 또한, *FL6*함수의 키 $KL_{6,2,2}$의 9비트를 "111111111"로 고정함으로서. 앞 절에서 제시한 5라운드 기본 포화 공격보다 더 나은 결과를 얻을 수 있다.

그림 1에 나타난 distinguisher를 2라운드부터 구성하면, 즉 2라운드 입력 값을 $Z^2=(C,A)$ 로 선택하면 4라운드 distinguisher $Z^6=(?,B)$를 얻을 수 있다. 이 4 라운드 distinguisher를 이용하여 5 라운드 포화 공격을 시도할 것이다.

이 공격에서는 *FL6*함수를 제외한 *FO6*에 쓰이는 부분키만을 찾을 것이다. 6라운드의 부분키 후보 $K=\{KO_{6,1}, KO_{6,2}, KI_{6,1,2}, KI_{6,2,2}\}$를 이용하여 5라운드 기본 공격과 같은 방법으로 암호문을 복호화 하면, *FO*함수 출력 9비트의 균일성질 유무를 판단할 수 있다.

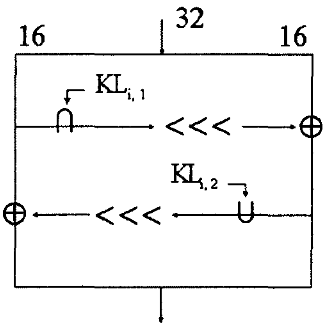

그림 4 *FL*함수

즉,

$$FO(CR, KO_6, KI_6)=(C_3', C_2', C_1', C_0')$$

라 할 때, $\bigoplus_{w_i\in((C_3'\wedge 3)\|C_2')} w_i=0$ 를 판단할 수 있다.

그림 4를 보면 알 수 있듯이,

$((C_3'\wedge 3)\|C_2')$와 *XOR* 되는 $KL_{6,2,2}$의 9비트 키를 "111111111"로 고정시키면,

$$\bigoplus_{w_i\in((Z_3^6\wedge 3)\|Z_2^6)} w_i$$
$$=\bigoplus_{w_i\in C_2'}\{w_i'\oplus 111111111\}=\bigoplus_{w_i\in C_2'} w_i'$$

이므로, 함수의 입력 값의 9비트 균일 성질이

그대로 유지됨을 알 수 있다.

선택 평문 집합 에 대하여, right key가 아니면서 50비트 부분키가 수식 (4)를 만족할 확률은 2^{-9}이다. 부분키 공간의 크기가 2^{50}이므로 right key를 확률적으로 올바른 키를 찾아내기 위해서는 적어도 7개의 선택 평문 집합이 필요하다.

이절에서 5라운드 포화 공격 복잡도는 2^{32}의 평문 집합 7개에 대하여 50비트의 부분키를 전수 조사하여 찾아내므로

$\frac{1}{5} \times 10 \times 2^{32} \times 2^{82} = 2^{115}$라 할 수 있다.

IV 결론

본 논문에서는 5라운드 KASUMI의 포화공격을 소개하였다. 공격 결과는 다음 표와 같다.

표 2 : KASUMI에 대한 포화공격의 결과

라운드	선택 평문수	공격 복잡도
5	10×2^{32}	2^{115}
향상된 5	7×2^{32}	2^{83}

위에서 본 표와 같이 전수조사보다 좋은 5라운드 KASUMI 포화공격을 했음을 알 수 있다. 본 논문의 공격 방법은 KASUMI와 비슷한 MISTY에도 적용가능하다.

참고문헌

[1] 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

[2] M. Masui, New Block Encryption Algorithm MISTY. In Fast Software Encrytion: 4th International Workshop, LNCS 1267, Sprinfer-Vrlag, 1997

[3] Hidema TANAKA, Chikashi ISHII, Toshimobu KANEKO. On the strength of KASUMI without FL functions against Higher Order Differential Attack. ICISC 2000, LNCS 2015, Springer-Verlag(2001) 14-21

[4] Yongjin Yeom, Sangwoo Park, Iljun Kim, On the Security of CAMELLIA against the Square Attack, LNCS

[5] L.R. Knudsen, D. Wagner, Integral Cryptanalysis, Fast Software Encryption, Springer Verag, 2002

[6] Mark Blunden, Adrian Escott, Relaed Key Attacks on Reduced Round KASUMI, FSE 2001, LNCS 2355, Springer-Verlag(2002) 277-285

[7] Ulrich Kuhn, Crypanalysis of Reduced-Round MISTY, EUROCRYPT 2002, LNCS 2045, Springer-Verlag(2001) 325-339

[8] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems. In journal of cryptology, (4), 1991.