情報保護學會論文誌
第11券 第4號, 2001. 8

3GPP 블록 암호의 S-box 안전성 분석

장 구 영*, 강 주 성*, 이 옥 연*, 정 교 일*

An analysis on the S-boxes of block ciphers in 3GPP

Ku-Young Chang*, Ju-Sung Kang*, Okyeon Yi*, Kyo-il Chung*

요 약

비동기식(W-CDMA) 3세대 이동통신의 3GPP는 무선 구간에서의 데이터 기밀성과 무결성을 제공하기 위하여 블록 암호 KASUMI에 기반한 f8과 f9 알고리즘을 제안했다. 또한, 3GPP 인증 및 키 생성 함수들에 대한 예로써 블록 암호 Rijndael에 기반한 Milenage 알고리즘을 제안했다. 따라서 3GPP 알고리즘의 안전성을 분석하기 위해서는 핵심 알고리즘인 KASUMI와 Rijndael의 안전성 분석이 선행되어야 한다. 블록 암호의 여러 구성 요소들 중에서 S-box는 가장 기본적인 안전성 요인들이 함축된 함수로 볼 수 있으므로 본 논문에서 우리는 KASUMI와 Rijndael의 S-box를 비교 분석한다. 더우기 KASUMI S9-box의 AC 및 SAC특성이 좋지 않지만, S7-box와 S9-box를 포함하고 있는 KASUMI FI 함수의 AC는 Rijndael S-box의 AC와 같고, KASUMI FI 함수의 SAC은 Rijndael S-box의 SAC과 비교해 좋다는 사실을 규명한다.

ABSTRACT

3GPP proposed f8 and f9 algorithms based on the block cipher KASUMI to provide the data confidentiality and integrity over a radio access link for IMT-2000(W-CDMA). Also 3GPP proposed Milenage algorithm based on the block cipher Rijndael to provide an example set for 3GPP authentication and key generation functions. In order to analyze the security of 3GPP algorithms, we must go ahead an analysis of security of KASUMI and Rijndael. Since S-box is an important point of security of block cipher, in this paper we analyze the S-boxes of KASUMI and Rijndael and compare the S-boxes of KASUMI with the S-box of Rijndael. Although KASUMI S9-box is bad for AC and SAC, we find that AC of KASUMI FI function containing S7-box and S9-box is equal to AC of Rijndael S-box and SAC of KASUMI FI function is better than SAC of Rijndael S-box.

keyword : *3GPP, Milenage, KASUMI, Rijndael, S-box*

Ⅰ. 서 론

비동기 3세대 이동통신의 3GPP(3rd Generation Partnership Project)에서는 민감한 정보에 대한 보호를 위해 9개의 암호 알고리즘을 요구하고 있다. 그 중 2개는 무선 구간에서의 데이터 기밀성을 위한 암호화 알고리즘 f8과 데이터 무결성을 위한 MAC(Message Authentication Code) 알고리즘 f9이다. f8과 f9는 블록 암호 KASUMI에 기반하여 만들어졌으며, 3GPP에 의해 표준화되었다. KASUMI는 ETSI(European Telecommunications Standards Institute) SAGE(Security Algorithms Group of Experts)에 의해 블록 암호 MISTY1이 개선되어 설계되었다. 나머지 7개는 인증 및 키 생성에 관한 알고리즘으로 표준화되어 있지 않다. 그러나 ETSI SAGE는 인증 및 키 생성 함수의 예로써

* 한국전자통신연구원 정보보호기술연구본부(jang1090, jskang, oyyi, kyoil)@etri.re.kr

f1, f1*, f2, f3, f4, f5, f5*를 설계하여 추천하고 있다. 이를 Milenage 알고리즘이라고 부른다. Milenage 알고리즘은 최근 차세대 미국 표준 암호 알고리즘 AES(Advanced Encryption Standard)로 선정된 Rijndael에 기반을 두고 있다. 따라서 3GPP의 9개 알고리즘의 안전성을 분석하기 위해서는 핵심 알고리즘인 KASUMI와 Rijndael의 안전성 분석이 선행되어야 한다.

대부분의 현대 블록 암호 알고리즘은 혼동(confusion)과 확산(diffusion)효과를 주기 위하여 대치(substitution) 단계와 치환(permutation) 단계를 포함하고 있다. 대치 단계는 입력을 몇 개의 작은 블록으로 구분한 후 각각의 소블록들에 S-box라 부르는 비선형 변환을 적용하여 출력 값을 얻는 과정으로 혼동 효과를 주기 위한 단계이다. 치환 단계는 대치 단계의 출력인 각각의 S-box 출력 값을 전체 블록에 골고루 분산시키기 위한 과정으로 확산 효과를 주는 구성 요소이다.

블록 암호 알고리즘을 설계할 때, 대부분의 경우 메모리 요구 조건 때문에 4×4, 8×8 등 작은 크기의 S-box를 대치 단계에서 사용하기 때문에 S-box가 가지는 암호학적 특성은 블록암호의 안전성에 중요한 요소가 된다. 대부분의 블록 암호에 대한 공격은 S-box의 약점을 이용해 이루어진다. 그러므로, 블록 암호에 대한 안전성을 검증하기 위해서는 S-box가 잘 설계되었는지 조사하는 것은 필수적이다.

Kavut와 Yücel[6]은 Rijndael S-box에 대한 Avalanche 특성, Strict Avalanche 특성, 비트 독립 특성(Bit Independence Criterion), 비선형성(nonlinearity), XOR 분포를 조사하였고, 그것을 Safer K-64에 사용된 두 개의 S-box와 비교하였다. 우리는 이 논문에서 KASUMI S-box의 위와 같은 5개 기준을 조사하고, Rijndael에 대한 조사를 확인해본다. 특히 KASUMI의 S9-box 경우 Avalnache 특성이나 Strict Avalanche 특성이 상당히 좋지 않음을 알 수 있다. 그러나 KASUMI S7-box와 S9-box를 포함하고 있는 KASUMI FI 함수의 Avalnache 특성은 Rijndael S-box의 Avalnache 특성은 같고, Strict Avalanche 특성은 Rijndael S-box보다 더 좋다는 사실을 밝힘으로써 KSAUMI의 FI 함수는 S9-box의 약점을 상쇄시킴을 확인한다. 또, 위의 기준 이외에도 KASUMI와 Rijndael S-box의 선형 구조와 대수적 차수를 조사한다.

Ⅱ. KASUMI 및 Rijndael에 사용된 S-box

2.1 KASUMI

KASUMI는 3GPP 기밀성 및 무결성 알고리즘인 f8과 f9에 들어가는 핵심 블록 암호 알고리즘으로 차분 공격(differential cryptanalysis)과 선형 공격(linear cryptanalysis)에 대하여 강한 내성을 갖도록 하기 위해 블록 암호 MISTY1을 개선하여 설계하였다. KASUMI의 구조는 블록 크기 64비트와 키 길이 128비트를 갖고 있는 Feistel 구조 블록 암호로서 다음과 같은 3단계로 분류할 수 있다.

(1) KASUMI는 두 개의 라운드 치환 FO와 FL을 포함하는 8라운드 Feistel 구조를 갖는 64비트 치환이다.
(2) FO 함수는 라운드 치환 FI를 포함하는 3라운드 MISTY-형 변환으로 구성된 32비트 치환이다.
(3) FI는 7×7 S-box인 S7-box와 9×9 S-box인 S9-box를 포함하는 4라운드 불균형 MISTY-형 변환으로 구성된 16비트 치환이다.

KASUMI S7-box는 유한체 $GF(2^7)$ 위에서 정의된 함수 $x \mapsto x^{81}$ 의 선형변환이다. 지수 81은 Kasami[5]에 의해 정의된 지수들의 집합에 포함되어 있다. $n=2m+1,\ 2 \le k \le m,\ \gcd(k,m)=1$일 때 $d \equiv 2^{2k}-2^k+1 \pmod{2^n-1}$을 고려하자. $d^*=2^t d \pmod{2^n-1}$을 만족하는 t가 존재할 때, 이러한 d^*들의 모임을 Kasami 지수(exponent)라고 부른다. $81=2^6+2^4+1 \equiv 2^1(2^4-2^2+1) \pmod{2^7-1}$이기 때문에 81은 $k=2$인 Kasami 지수이다.

KASUMI S9-box는 유한체 $GF(2^3)$ 위에서의 함수 $x \mapsto x^5$ 과 선형 출력 변환(linear output transformation)의 합성으로 이루어져있다.

2.2 Rijndeal

3GPP는 인증 및 키 생성에 대한 알고리즘으로 차세대 미국 표준 암호 알고리즘인 AES로 채택된 Rijndael에 기반한 Milenage 알고리즘을 설계하여 추천하고 있다. Rijndael의 키 길이는 AES의 요구에 따라 128, 192, 256 비트를 갖도록 정의되어 있다. 그러나 Milenage 알고리즘에 사용되는 블록

암호 Rijndael은 블록 크기 128비트와 키 길이 128비트를 갖고 있는 SPN(Substitution-Permutation Network)구조이다. Rijndael은 대치 단계에 한 종류의 8×8 S-box 16개를 사용하도록 설계되어 있다.

그리고 이 8×8 S-box는 $GF(2^8)$ 위에서 정의된 함수 $x\mapsto x^{-1}$ (단, $0\mapsto0$)와 선형 출력 함수와의 합성으로 구성되어있다.

2.3 S-box 설계 기준

블록 암호의 일반적인 공격은 S-box 내의 어떤 약점을 조사함으로써 이루어진다. 따라서 새로운 공격이 도입되면 S-box의 새로운 기준이 도입된다. 예를 들어 블록 암호의 가장 강력한 공격법 중 하나로 알려진 차분 공격이 도입된 이후로 S-box 설계 기준에 XOR 분포 조사 항목이 추가되었다. 우리는 KASUMI와 Rijndael의 S-box의 안전성을 분석하기 위해 다음 7가지의 기준에 대하여 조사할 것이다.

(1) Avalanche 특성
(2) Strict Avalanche 특성
(3) 비트 독립 특성(BIC)
(4) 대수적 차수
(5) 선형 구조
(6) XOR 분포
(7) 비선형성

Ⅲ. S-box 안전성 분석

$n\times k$ S-box는 $Z_2^n\to Z_2^k$로 가는 함수로써 $S(x)=(f_1(x), f_2(x), \cdots, f_k(x))$이다. 여기에서 $n\geq k$ 이고, $f_j: Z_2^n\to Z_2$ 이다. 2.1과 2.2에서 보듯이 KASUMI와 Rijndael의 S-box는 유한 체(finite field) 위에서 정의된 x의 지수함수로 되어 있다. 이 지수 함수들은 수학적으로 유사한 성질을 갖고 있으므로 우리는 다음에 나오는 7가지 방법에 의해 KASUMI와 Rijndael의 S-box들을 비교해 볼 것이다.

3.1 AC 및 SAC 특성

Completeness는 Kam과 David[4]에 의해 처음 도입되었다. 임의의 $(i, j | 1\leq i\leq n, 1\leq j\leq k)$에 대하여, 입력 쌍 x, y가 단지 i번째 한 비트 다를 때 적어도 출력 쌍 $S(x)$, $S(y)$의 j번째 비트가 다른 하나 이상의 입력 쌍이 존재하면 S를 completeness라고 부른다. 다시 말해 각각의 출력 비트가 모든 입력 비트에 의존할 때, 함수를 completeness라고 부른다.

Avalanche 개념은 Feistel[3]에 의해 도입되었다. Avalanche는 한 비트 차이가 나는 입력에 대한 출력의 변화를 조사하는 것이다. P_i가 P와 i번째 비트만 다른 입력일 때, 두 입력 P, $P_i\in Z_2^n$를 고려하자.

$$S(P)\oplus S(P_i)$$
$$=(f_1(P)\oplus f_1(P_i),\cdots,f_k(P)\oplus f_k(P_i))$$
$$W_{i,j}=\sum_{P\in Z_2^n} f_j(P)\oplus f_j(P_i)$$

[정의 1]

$K_{AC}(i)=\frac{1}{k\cdot 2^n}\sum_{j=1}^{k} W_{i,j}$라고 하자. 모든 $i\in\{1, \cdots, n\}$에 대하여 $K_{AC}(i)=1/2$이면 $n\times k$ S-box는 AC(Avalanche Criterion)를 만족한다고 한다.

AC를 만족한다는 것은 한 비트 차이가 나는 입력에 대하여 전체 출력의 정확히 반이 변한다는 것을 의미한다.

Webster와 Tavares[11]는 completeness와 AC의 개념을 결합해 SAC(Strict Avalanche Criterion)이라는 개념을 도입하였다.

[정의 2]

$K_{SAC}(i,j)=\frac{1}{2^n}W_{i,j}$라고 하자. 모든 $i\in\{1, \cdots, n\}$, $j\in\{1, \cdots, k\}$에 대하여 $K_{SAC}(i,j)=1/2$이면 $n\times k$ S-box는 SAC을 만족한다고 한다.

SAC을 만족한다는 것은 한 비트 차이가 나는 입력에 대하여 각각의 성분 함수 f_j의 출력의 반이 변한다는 것을 의미한다. SAC을 만족하면 AC를 만족한다는 것을 쉽게 알 수 있다.

실제 블록 암호의 S-box는 AC나 SAC을 만족하지 않을 수 있으므로 우리는 다음과 같은 오차를 정의할 수 있다.

$$\varepsilon_{AC}=\max_{1\leq i\leq n}|2K_{AC}(i)-1|$$

$$\varepsilon_{SAC}=\max_{\substack{1\leq i\leq n\\ 1\leq j\leq k}}|2K_{SAC}(i,j)-1|$$

여기에서 ε_{AC}는 AC 오차를, ε_{SAC}은 SAC 오차를 의미한다.

〔표 1〕~〔표 4〕는 KASUMI와 Rijndeal에 사용된 S-box 의 AC 및 SAC 특성과 관련된 조사 내용이다. 〔표 1〕~〔표 3〕까지의 (i, j)번째 원소는 $W_{i,j}$를 나타낸다.

〔표 1〕 KASUMI S7-box의 $W_{i,j}$조사

j \ i	1	2	3	4	5	6	7
1	64	64	72	64	64	64	64
2	64	64	64	72	64	64	64
3	64	64	64	64	64	72	64
4	64	64	64	64	72	64	64
5	72	64	64	64	64	64	64
6	64	72	64	64	64	64	64
7	64	64	64	64	64	64	72

〔표 2〕 KASUMI S9-box의 $W_{i,j}$조사

j \ i	1	2	3	4	5	6	7	8	9
1	256	256	256	256	256	256	512	256	256
2	256	256	512	256	256	256	256	256	256
3	256	256	256	256	256	512	256	256	256
4	512	256	256	256	256	256	256	256	256
5	256	256	256	256	512	256	256	256	256
6	256	256	256	512	256	256	256	256	256
7	256	512	256	256	256	256	256	256	256
8	256	256	256	256	256	256	256	256	512
9	256	256	256	256	256	256	256	512	256

〔표 3〕 Rijndael S-box의 $W_{i,j}$조사

j \ i	1	2	3	4	5	6	7	8
1	132	132	116	144	116	124	116	128
2	120	124	144	128	124	116	128	136
3	132	132	128	120	144	128	136	128
4	136	136	120	116	128	136	128	140
5	116	128	116	132	128	128	140	136
6	116	132	132	120	120	140	136	136
7	136	136	120	132	120	136	136	124
8	132	144	132	136	124	136	124	132

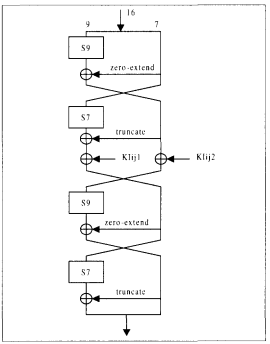
〔표 4〕 AC 및 SAC 조사

블록 암호 및 S-box	ε_{AC}	ε_{SAC}
Rijndael S-box	0.1250	0.0352
KASUMI S7-box	0.1250	0.0179
KASUMI S9-box	1	0.1111

〔표 4〕에 의하면, Rijndael S-box와 KASUMI S7-box에 비하여 KASUMI S9-box의 AC와 SAC의 오차 값이 좋지 않음을 알 수 있다. 그러나, KASUMI는 두 개의 S-box(S7-box, S9-box)를 FI 함수 내에 포함하고 있으므로 S9-box의 오차 값이 좋지 않다고 하더라도 전체 FI 함수의 오차 값이 좋다면 S9-box의 좋지 않은 특성은 상쇄되어 전체 KASUMI의 안전성에는 영향을 미치지 못할 것이다. 그러므로 FI 함수의 AC 및 SAC 특성을 조사해 볼 필요가 있다.

3.2 KASUMI FI 함수의 AC 및 SAC

〔그림 1〕에서 보는 바와 같이 KASUMI FI함수에는 키 KIij1과 KIij2가 들어가 있으므로 임의의 키에 대하여 AC 및 SAC 특성을 조사해야 한다. 우리는 KASUMI FI 함수를 16×16 S-box로 간주하여 다음을 정의한다.



〔그림 1〕 KASUMI의 FI 함수

$$W_{\max}^{FI} = \max_{K \in Z_2^{16}} \max_{1 \le i,j \le 16} W_{i,j}^{K}$$

$$W_{\min}^{FI} = \min_{K \in Z_2^{16}} \min_{1 \le i,j \le 16} W_{i,j}^{K}$$

$W_{i,j}^{K}$는 16비트 키 K가 고정되었을 때, $W_{i,j}$의 값이다.

$$\varepsilon_{AC}^{FI} = \max_{K \in Z_2^{16}} \varepsilon_{AC}^{K}$$

$$\varepsilon_{SAC}^{FI} = \max_{K \in Z_2^{16}} \varepsilon_{SAC}^{K}$$

ε_{AC}^{K}는 16비트 키 K가 고정되었을 때, ε_{AC}의 값이다.

[표 5] KASUMI FI 함수의 AC 및 SAC 조사

조사 내용	KASUMI FI 함수
$W_{\max}^{FI}$	33792
$W_{\min}^{FI}$	28672
ε_{AC}^{FI}	0.12500
ε_{SAC}^{FI}	0.01025

[표 5]에 의하면 FI 함수의 AC 및 SAC의 오차값이 Rijndael S-box의 AC와는 같고, Rijndael S-box의 SAC 오차 값보다 작다는 사실을 참고적으로 알 수 있다. 그런데 FI 함수는 16×16 이고 Rijndael S-box는 8×8 이므로 수치상의 비교는 큰 의미가 없다고 여겨진다. 하지만 KASUMI FI 함수는 S9-box의 AC 및 SAC의 나쁜 특성이 표출되지 않도록 잘 설계되어 있다는 것을 알 수 있다.

3.3 BIC 특성

BIC(Bit Independence Criterion)의 개념은 Webster과 Tavares[11]에 의해 도입되었다. BIC는 i번째 비트만 다른 두 개의 입력에 대하여 출력 $S(P) \oplus S(P_i)$의 성분들이 서로 독립인가를 조사하는 것이다. $d_j^{(i)} = f_j(P) \oplus f_j(P_i)$라고 하자.

[정의 3]

$$BIC_{j,m}^{(i)} = | corr(d_j^{(i)}, d_m^{(i)}) |$$

$$corr(A,B) = \frac{E[AB] - E[A] \cdot E[B]}{\sigma(A) \cdot \sigma(B)}$$

여기에서 $\sigma(A)^2 = E[A^2] - (E[A])^2$은 분산이고, $E(A)$는 A가 일어날 기대값이다.

[정의 4]

$$BIC(S) = \max_{\substack{1 \le i \le n \\ 1 \le j,\, m \le k,\, j \ne m}} BIC_{j,m}^{(i)}.$$

$BIC(S) \in [0,1]$ 이고, 0인 경우는 모든 성분들이 독립이라는 것이고, 가장 좋지 않은 경우에 $BIC(S)$의 값은 1이 된다.

[표 6] BIC 조사

블록 암호 및 S-box	$BIC(S)$
Rijndael S-box	0.1341
KASUMI S7-box	0.1260
KASUMI S9-box	0

[표 6]에서 알 수 있듯이 KASUMI S9-box는 AC 및 SAC 성질은 좋지 않으나, BIC 성질은 가장 좋은 값인 0을 갖는다는 것을 알 수 있다.

3.4 대수적 차수

[정의 5]

부울 함수 $f : Z_2^n \to Z_2$가 다음과 같이 쓰여질 때, 대수적 정규 표현(Algebraic Normal Form)이라 부른다.

$$f(x) = a_0 \oplus \sum_{1 \le i \le n} a_i x_i \oplus \sum_{1 \le i < j \le n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$$

이때, 계수가 0이 아닌 것의 차수 중 최대값을 대수적 차수(algebraic degree)라고 하고, $\deg(f)$로 표시한다. 그리고, $S(x) = (f_1(x), \cdots, f_k(x))$의 차수 $\deg(S)$는 $\max_{1 \le j \le k} \deg f_j(x)$로 정의한다.

[표 7] 대수적 차수

블록 암호 및 S-box	deg(S)
Rijndael S-box	7
KASUMI S7-box	3
KASUMI S9-box	2

〔표 7〕에 의하면 KASUMI S7-box와 S9-box의 대수적 차수가 낮다는 것을 알 수 있다. 대수적 차수가 낮은 경우 고차 차분 공격(Higher Order Differential Attack)에 약하다는 것이 알려져 있다. 이를 이용하여 TANAKA-ISHII- KANEKO[10]는 FL 함수가 없는 KASUMI 4-라운드를 1,416개의 선택 평문(chosen plaintext)을 사용하여 공격하였다. 그러나 KASUMI는 8-라운드로 설계되었기 때문에 현재까지 전체의 안전성에는 문제가 없는 것으로 보인다.

3.5 선형 구조

〔정의 6〕

$u \in Z_2^n - \{0\}$에 대하여 $f_u(x) = \langle S(x), u \rangle$를 고려하자. 여기에서 $\langle S(x), u \rangle$는 $S(x)$와 u의 Z_2 위에서의 내적이다. 0이 아닌 w에 대하여 $f_u(x) \oplus f_u(x \oplus w)$의 값이 상수일 때, 함수 $f_u(x)$는 w에 대하여 선형 구조를 갖는다고 한다. 선형 구조는 SAC과 상반된 개념으로 S-box 내에 일어나지 않도록 설계해야 한다.

〔표 8〕 선형 구조

블록 암호 및 S-box	선형 구조를 갖는 원소의 수
Rijndael S-box	0
KASUMI S7-box	0
KASUMI S9-box	511

〔표 8〕에 의하면 KASUMI S9-box는 511개의 선형 구조를 가진다. 이것은 KASUMI S9-box의 SAC가 좋지 않다는 사실과 일치한다. 우리는 KASUMI FI 함수의 SAC가 좋다는 사실로부터 KASUMI FI 함수가 선형 구조를 적게 가질 것이라는 사실을 추측을 할 수 있다. 3GPP에서의 분석에 의하면 KASUMI FI 함수는 선형 구조를 갖지 않는다.[12] 즉 KASUMI는 S9-box의 선형 구조가 FI 함수로 전파되지 않도록 잘 설계되어 있다는 것을 알 수 있다.

3.6 XOR 분포

Biham과 Shamir[12]는 블록 암호 알고리즘의 공격 중 하나인 차분 공격을 도입하였다. 이것은 입력의 변화에 대한 출력의 변화를 추적하여 키에 대한 정보를 확률적으로 유추하는 기법이다. 차분 공격을 사용하기 위해서는 다음과 같은 집합이 필요하다.

$$D_S(a, b) = \{P \in Z_2^n \mid S(P \oplus a) \oplus S(P) = b\}$$

〔정의 7〕

$a \in Z_2^n$, $b \in Z_2^n$이고, $\delta_S(a, b) = \#D_S(a, b)$이라 하자. 그때에

$$\Delta_S = \max_{a \neq 0,\ b} \delta_S(a, b)$$

로 정의한다.

〔정의 8〕

우리는 $\Delta_S \geq 2$라는 것을 알 수 있고, $\Delta_S = 2$를 만족할 때 S를 APN(Almost Perfect Nonlinear)이라고 부른다.

XOR 표는 2^n개의 행과 2^k개의 열로 구성되어 있고, 행에는 정의 7의 a를 표시하고 열에는 b를 표시한다. XOR 표 내의 a행 b열에는 $\delta_S(a, b)$를 표시한다. XOR 표는 차분 공격에 대한 블록 암호의 안전성에 대한 정보를 표시하고 있다. 차분 공격의 효율은 $\delta_S(a, b)$에 의해 측정되기 때문에 Δ_S의 값이 작을수록 S-box는 차분 공격에 대하여 더 좋은 내성을 가지게 된다.

유한체 $GF(2^n)$ 위에서 정의된 함수 x^e은 차분 공격에 대한 관점에서 우수한 특성을 가진다. 이 특성은 e에 따라 다르며 KASUMI S-box들과 Rijndael S-box의 지수 e에 대하여 현재까지 알려진 결과를 종합하면 다음과 같다.

〔정리 1〕

e가 Kasami 지수이면, $\Delta_S = 2^t$이다.[5]

〔정리 2〕

$e = 2^t + 1$이고, $\gcd(k, n) = t$이면 $\Delta_S = 2^t$이다. 또 $e = -1$이고 n이 짝수이면 $\Delta_S = 4^t$이고, n이 홀수이면 $\Delta_S = 2^t$이다.[8]

〔표 9〕 Δ_S 조사

블록 암호 및 S-box	Δ_S
Rijndael S-box	4
KASUMI S7-box	2
KASUMI S9-box	2

[표 9]에 의하면 잘 알려진 정리들과 실제 XOR 표를 통해 구한 Δ_S 값이 일치함을 알 수 있다. 게다가 KASUMI S-box들은 APN이기 때문에 차분 공격에 대해 강한 내성을 갖고 있다는 것을 알 수 있다.

3.7 비선형성

Matsui[6]는 입력 블록과 출력 블록을 선형적으로 근사시켜 키에 대한 정보를 유추하는 선형 공격을 도입하였다. 차분 공격의 경우와 유사하게 다음과 같은 집합을 정의한다.

$$L_S(a,b)=\{P\in Z_2^n \mid \langle a,P\rangle=\langle b,S(P)\rangle\}$$

[정의 8]

$a\in Z_2^n$, $b\in Z_2^n$이고,

$$\lambda_S(a,b)=\#L_S(a,b)-|Z_2^n|/2 = \#L_S(a,b)-2^{n-1}$$

이라 하자. 그때에

$$\Lambda_S=\max_{a,b\neq 0}|\lambda_S(a,b)|,\quad p_S=\Lambda_S/2^n$$

라고 정의한다.

선형 공격의 효율은 $L_S(a,b)$와 $|Z_2^n|/2$사이의 불일치 값 $\lambda_S(a,b)$에 의해 측정되기 때문에 Λ_S의 값이 작을수록 S-box는 선형 공격에 대하여 더 좋은 내성을 가지게 된다. 다음 [표 10]은 $a\in Z_2^n$, $b\in Z_2^n-\{0\}$인 경우에 대하여 조사한 것이다.

[표 10] Λ_S 조사

블록 암호 및 S-box	$L_S(a,b)$의 최소값	$L_S(a,b)$의 최대값	Λ_S	p_S
Rijndael S-box	112	144	16	$1/2^4$
KASUMI S7-box	56	72	8	$1/2^4$
KASUMI S9-box	240	272	16	$1/2^5$

Ⅳ. 결 론

본 논문에서는 3GPP에서 요구하고 있는 정보보호 알고리즘에 핵심으로 들어가는 KASUMI와 Rijndael의 S-box를 7가지 측면에서 분석하였다.

KASUMI S9-box의 경우 AC 및 SAC 특성이 좋지 않았고 선형 구조를 갖고 있었으나, S7-box와 S9-box를 포함하는 KASUMI FI 함수의 AC 특성은 Rijndael S-box의 AC 특성과 같고, KASUMI FI 함수의 SAC 특성은 Rijndael의 S-box와 비교해 좋았고, FI 함수는 선형 구조를 갖고 있지 않기 때문에 전체적인 안전성에는 큰 문제가 없는 것으로 여겨진다. 따라서 KASUMI는 S9-box의 약점이 FI 함수로 확산되지 않도록 잘 설계되어 있다는 것을 알 수 있다. 또, KASUMI S-box들의 대수적 차수가 낮기 때문에 Higher Order Differential Attack에 공격당할 위험이 있으나, 현재까지 4-라운드 공격에만 성공하였기 때문에 8-라운드 KASUMI의 안전성은 문제가 없다고 보여진다.

KASUMI의 S-box들은 Rijndael의 S-box에 비하여 BIC에서 좋은 성질을 보이고 있고, 차분 공격 관점에서는 APN(Almost Perfect Nonlinear)이므로 상당히 잘 설계되어 있다고 볼 수 있다. 나머지 관점에 대해서는 KASUMI와 Rijndael의 S-box는 비슷한 결과가 나옴을 알 수 있다.

참 고 문 헌

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like Cryptosystems", Advance in Cryptoology-CRYPTO'90, LNCS 537, Springer-verlag, pp. 2~21, 1990.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, Vol. 4, No. 1, pp. 3~72, 1991.

[3] H. Feistel, "Cryptography and computer privac", Scientific American, Vol. 228, No. 5, pp. 15~23, May 1973.

[4] J. B. Kam and G. I. Davida, "Structured design of substitution-permutation encryption networks", IEEE Transactions on Computers, Vol. C-28, No. 10, pp. 747~753, October 1979.

[5] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes", Information and Control, Vol. 18, pp. 369~394, 1971.

[6] S. Kavut and M. D. Yücel, "On some cryptographic Properties of Rijndael", MMM-ACNS 2001, LNCS 2052, pp. 300~311, 2001.

[7] M. Matsui, "Linear cryptanalysis method for DES cipher", Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag, pp. 386~397, 1994.

[8] K. Nyberg, "Differentially uniform mappings for cryptography", Advances in Cryptology-EURO CRYPT'93, LNCS 765, Springer-Verlag, pp 55- 64, 1994.

[9] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, 28, pp. 656~715, 1949.

[10] H. Tanaka, C. Ishii, and T. Kaneko, "On the strength of KASUMI without FL functions against Higher Order Differential Attack", ICISC 2000, LNCS 2015, pp. 14~21, December 2000.

[11] A. F. Webster and S. E. Tavares, "On the design of S-boxes", Advances in Cryptology-Proceedings of CRYPTO '85, Springer-Verlag, pp. 523~534, 1986.

[12] ETSI/SAGE, Specification of the 3GPP Confidentiality and Integrity Algorithms, available at http://www.etsi.org/dvbandca/3GPP/3gppspecs.htm.

〈著者紹介〉

장 구 영 (Ku-Young Chang)
1995년 2월 : 고려대학교 이과대학 수학과(학사)
1997년 2월 : 고려대학교 수학과(석사)
2000년 8월 : 고려대학교 수학과(박사)
2000년 12월~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 정보보호 이론, 이동통신 정보보호

강 주 성 (Ju-Sung Kang)
1989년 2월 : 고려대학교 이과대학 수학과(학사)
1991년 2월 : 고려대학교 수학과(석사)
1996년 2월 : 고려대학교 수학과(박사)
1997년 12월~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 암호 이론

이 옥 연 (Okyeon Yi)
1988년 2월 : 고려대학교 이과대학 수학과(학사)
1990년 2월 : 고려대학교 수학과(석사)
1996년 8월 : University of Kentucky(박사)
1999년 7월~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 이동통신 정보보호, 컴퓨터 보안

정 교 일 (Kyo-il Chung)
1981년 2월 : 한양대학교 전자공학과(학사)
1993년 8월 : 한양대학교 산업대학원 전자계산학과(석사)
1997년 8월 : 한양대학교 전자공학과(박사)
1981년 12월~현재 : 한국전자통신연구원 정보보호기술연구본부 부장/책임연구원
〈관심분야〉 IC Card, Security, Biometry, 정보전, 신호처리