블록암호 알고리즘 PACA에 대한 차분 분석

성 재 철*, 현 진 수*, 천 동 현*, 전 길 수*, 강 성 우*

*한국정보보호진흥원 암호기술팀

Differential Cryptanalysis of PACA

Jaechul Sung*, Jinsu Hyun*, Donghyeon Cheon* Kilsoo Chun*, Sungwoo Kang*

*Cryptographic Technology Team, KISA

요 약

본 논문에서는 블록암호 알고리즘의 분석 중에 가장 널리 사용되고 있는 차분 분석법을 이용하여 정부전자관인인증체계(GPKI)가 지원하는 암호화용 알고리즘중의 하나인 블록암호 알고리즘 PACA에 적용하여 분석하였다 [10,8]. 그 결과, 7-라운드의 차분 특성 확률이 2^{-120}이 되는 특성을 발견하였다. 이 차분 특성을 이용하여, 8-라운드 PACA에 대해 전수조사보다 빠른 공격법을 소개한다.

I. 서론

블록암호 알고리즘에 분석 법 중 현재까지 가장 널리 적용되고 사용되는 것은 차분 분석법(Differential Cryptanalysis)이다 [3]. 1990년대 초반 이 공격 법이 소개된 후, 이 방법을 이용하여 여러 블록암호 알고리즘들이 효과적으로 분석되었다. 또한, 차분 분석을 보다 발전시킨 공격법인 조건부 차분 공격 [1], 부정 차분 공격 [4], 불능 차분 공격 [2], 고계 차분 공격 [4,5], 부메랑 공격 [7] 등이 소개되었다.

차분 분석법이 블록암호 분석에 효과적으로 이용된 후, 1990년 중반 이후에 개발된 블록암호 알고리즘들은 차분 분석에 안전하도록 설계되고 있다.

블록암호 알고리즘 PACA [8]는 정부전자관인인증체계(GPKI)가 지원하는 암호화용 알고리즘 중의 하나인 블록암호 알고리즘이다. PACA는 (16+4t)라운드 Feistel 구조로서 (128+64t)-비트의 평문을 입력받아 (128+64t)비트 키를 사용하여 암·복호화 연산을 수행하는 가변 블록암호 알고리즘이다. 현재까지 이 알고리즘의 안전성에 대한 어떠한 분석도 이루어지지 않은 실정이다.

본 논문에서는 t=0인 경우, 즉 128-비트의 블록길이와 128-비트의 키 길이를 갖는 16-라운드 PACA에 대해 차분 분석을 수행한다. 우선, 라운드 함수 F에 대한 구조적 특징을 연구하여 한 라운드의 확률 2^{-30}의 차분 특성을 발견하였고, 이를 기본으로 하여 7-라운드 2^{-120}의 확률의 차분 특성을 구성하였다. 이 차분 특성으로 차분 공격의 기본 방법인 IR 공격을 적용하여 8-라운드 PACA에 대한 분석 방법을 소개한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 블록암호 알고리즘 PACA에 대한 소개를 하고 3장에서는 7-라운드 차분 특성을 소개한다. 4장에서는 7-라운드 차분 특성을 이용하여 8-라운드 PACA에 대해 전수조사보다 빠른 공격법을 소개한다. 마지막으로 5장에서는 본 논문의 결과와 향후 연구과제에 대해 소개한다.

II. 블록암호 알고리즘 PACA 소개

PACA는 (128+64t)-비트의 가변 길이에 모두 적용 가능한 알고리즘이다. 전체적인 구조는 Feistel 구조로서 (128+64t)-비트의 평문을 입력받아 (128+64t)비트 키를 사용하여 암·복호화 연산을 수행한다. 본 논문에서는 현재 가장 보편적으로 사용되고 있는 블록 및 키의 길이가 128-비트인 경우(t=0)만을 살펴본다.

본 논문의 분석에는 키 스케쥴 부분은 이용하지 않으므로 생략한다.

1. 연산 기호의 정의

블록암호 알고리즘에 PACA에 사용되는 연산을 다음과 같이 정의한다.

- $a \oplus b$: a와 b의 비트별 XOR
- $a \boxplus b$: a와 b의 법 2^{16}위에서의 덧셈
- $a \odot b$: a와 b의 법 $2^{16}+1$위에서의 곱셈

2. 전체 구조

PACA의 전체 구조는 Feistel 구조이고 라운드 함수 F는 64-비트의 입출력을 내는 함수이다. 다음의 그림 1은 PACA의 전체구조를 나타내고 있다. 각 라운드에 사용된 라운드 키 SK^i는 96-비트이다.

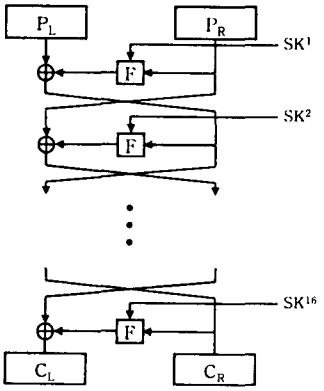

그림 1. PACA의 전체 구조도

3. 라운드 함수 F

이제, PACA의 라운드 함수 F에 대해 살펴보자. PACA의 라운드 함수의 입출력 길이는 64-비트이고 총 96-비트의 라운드 키 SK^i와 64-비트의 키에 의해 정의된 상수 Q^i에 의해 정의된다. 다음의 그림 2는 라운드 함수 F를 도식화 한 것이다.

각 라운드에 사용된 라운드 키 $SK_1, SK_2, SK_3, SK_4, SK_{5,1}, SK_{5,1}$는 각각 16-비트이다. 또한 각 Q_i는 키에 의해 정의된 16-비트의 상수이다.

라운드 함수 F에서 사용된 S는 16-비트의 입출력을 갖는 S-박스이다. 이 S-박스는 $GF(2^{16})$에서 x^{-1}의 아핀 변환에 의해 생성된다. 이러한 설계 방식은 최근의 블록암호에의 confusion 효과를 주는 방식에 주로 사용되는 설계방식으로 AES나 SEED 등의 S-박스 설계에도 사용되었다.

하지만, AES [6]나 SEED [9] 등은 S-박스의 메모리 량과 구현의 효율성을 위해 8-비트의 입출력을 갖는 S-박스를 사용하였으나, PACA에서는 16-비트의 입출력을 갖는 S-박스를 사용하였다. 이러한 S-박스의 구현을 위해서는 총 128 Kbyte의 메모리가 요구되어진다. 이러한 메모리 요구량은 기존의 다른 블록암호 알고리즘에 비해 비교적 많은 메모리 요구량으로 스마트 카드와 같이 적은 메모리를 가지는 환경에서는 사용이 제한되어질 수 있다는 단점을 가진다.

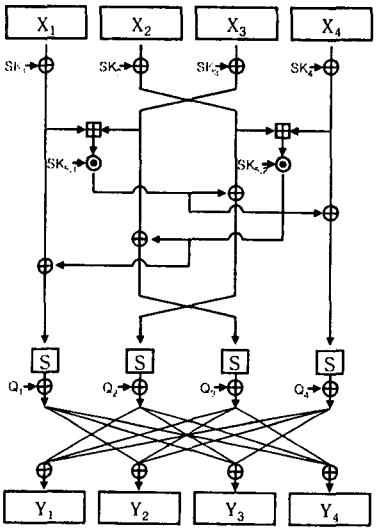

그림 2. PACA의 라운드 함수 F

III. 7-라운드 차분 특성

이 장에서는 PACA의 라운드 함수의 분석하고, 이를 이용하여 7-라운드 PACA의 차분 특성을 소개한다.

1. 라운드 함수 F의 분석

PACA의 라운드 함수의 두드러진 특징중의 하나는 차분 분석등의 적용을 어렵게 하기 위해 블록암호 알고리즘 IDEA에서 쓰인 법 $2^{16}+1$위에서의 곱셈($\odot$) 연산을 사용한 것이다. 이는 라운드의 키가 0이 아닌 경우 차분 특성의 구성을 어렵게 한다.

또한 S-박스를 x^{-1}의 아핀 변환으로 사용함으로써, 임의의 0이 아닌 입력 차분 α에 대해 어떠한 출력 차분 β가 나오는 확률 $DP(\alpha \rightarrow \beta)$이 최대 2^{-14}이 되도록 하였다(대부분의 경우의 확률 값은 2^{-15}이다).

이러한 두 가지의 특징으로 한 라운드의 차분 특성식의 구성을 어렵게 하였고 그 특성식에 대한 확률 값도 작게 나오게 하는 효과를 얻고자 하였다.

하지만, 이러한 노력은 각 블록 단위 결합 방식과 diffusion의 단순성 때문에 라운드 함수에 사용된 연산 량에 비해 큰 효과를 발휘하지는 못한다.

그러면 이제 라운드 함수에 대한 효과적인 특성식을 찾아보자. 우선 각 라운드의 입력 차분 값을 $(\Delta X_1, \Delta X_2, \Delta X_3, \Delta X_4)$이라 놓고 출력 차분 값을 $(\Delta Y_1, \Delta Y_2, \Delta Y_3, \Delta Y_4)$이라 놓자.

우선 4개의 블록 중 하나의 블록 차분만 0이 아니라고 하면 diffusion으로 인해 3개의 S-박스 입력 차분 중 3개의 블록이 0이 아닌 값이 된다. 즉, active S-박스의 수가 3이 된다. 따라서 한 라운드의 차분 특성식의 값은 2^{-42}보다 작게 된다. 이는 효과적인 차분 특성식으로 사용될 수 없다.

라운드 함수 F의 입력 차분을 $(\alpha,0,\alpha,0)$로 놓자. 첫 번째 블록과 세 번째 블록의 차분이 덧셈 연산 후 $SK_{5,1}$과 곱셈 연산을 하므로 $\gamma = SK_{5,1} \cdot (\alpha+\alpha)$가 된다. 이 차분은 두 번째 블록과 네 번째 블록에 XOR된다. 따라서 S-박스 입력 차분은 $(\alpha,\gamma,\alpha,\gamma)$이 된다. 이 차분을 그대로 사용하면 active S-박스의 수가 4가 된다.

여기서 γ의 값이 0이 되게 할 수 있다면 active S-박스의 수를 2로 줄일 수 있다. 이렇게 하기 위해서는 두 입력 차분의 합, 즉 $\alpha+\alpha$의 값을 0으로 만들어 주어야 한다. α가 0이 아닌 비트가 최상위 비트에만 존재한다면 쉽게 $\alpha+\alpha$이 0이 되게 만들 수 있다 (즉, $\alpha = 0x8000$). $\alpha = (\alpha_{15}, \cdots, \alpha_0)$가 최상위 비트를 제외한 부분의 0이 아닌 비트의 수를 r이라고 하면 $\alpha+\alpha$이 0이 될 확률은 대략 2^{-r} 정도가 된다.

이제부터 $\alpha = 0x8000$이라 하고, F 함수의 입력 차분을 $(\alpha,0,\alpha,0)$로 놓고, 출력 차분 역시 $(\alpha,0,\alpha,0)$으로 놓자. S-박스의 차분 분포에서 입력 α에 대한 출력 α의 차분 확률을 2^{-15}로 가정한다면 다음과 같은 라운드 함수 F에 대한 차분 특성 확률을 얻을 수 있다.

$$DP_F((\alpha,0,\alpha,0) \rightarrow (\alpha,0,\alpha,0)) = 2^{-30} \quad \text{(Type1)}$$

또한, 라운드 함수 F의 연산의 대칭성을 이용한다면 위와 비슷한 방법으로 다음을 얻을 수 있다.

$$DP_F((0,\alpha,0,\alpha) \rightarrow (0,\alpha,0,\alpha)) = 2^{-30} \quad \text{(Type2)}$$

우리는 이러한 한 라운드 특성식을 다음에 소개할 7-라운드 특성식과 이를 이용할 8-라운드 공격에 사용할 것이다.

2. 7-라운드의 차분 특성식

앞 절에서 구성한 한 라운드 차분 특성식은 입력 차분과 출력 차분이 같은 값이므로 연속적인 라운드에 적용하기에는 아주 적합한 특성식이다. 다음은 확률 2^{-120}인 7-라운드 차분 특성식을 나타낸 것이다.

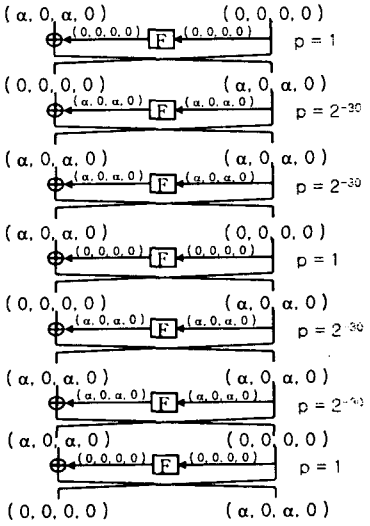

그림 3. PACA의 7-라운드 차분 특성식

IV. 8-라운드 PACA에 대한 차분 공격

이 장에서는 앞 장에서 구성한 확률 2^{-120}의 7-라운드 차분 특성식을 이용하여 차분 분석법의 1R 공격을 적용하여 8-라운드 PACA에 대한 공격법을 소개한다.

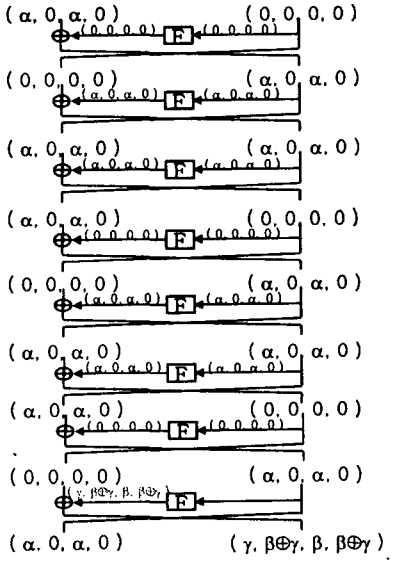

그림 4. 8-라운드 PACA의 차분 공격

우선 차분이 $(\alpha,0,\alpha,0,0,0,0,0)$인 선택 평문 쌍 (P_1,P_2)에 대한 암호문 쌍 (C_1,C_2)을 얻는다($\alpha=0x8000$). 이 암호문 쌍 중 임의의 0이 아닌 β와 γ에 대해, 차분이 $(\alpha,0,\alpha,0,\gamma,\beta\oplus\gamma,\beta,\beta\oplus\gamma)$ 꼴이 되는 지를 판단한다. 임의의 암호문 쌍이 이러한 꼴을 만족할 확률은 2^{-96}이다. 이러한 꼴을 만족하는 암호문 쌍에 대해 (이러한 과정을 필터링이라 부른다[3].), 8-라운드의 SK_1과 SK_3의 후보 2^{32}를 추측하여 7라운드의 왼쪽 64-비트의 차분이 $(0,0,0,0)$을 만족하는 지를 판단한 후, 이러한 차분이 만족하면 올바른 키 후보로 카운트한다. 이러한 일련의 과정을 반복하여 8-라운드 키 SK_1과 SK_3를 찾아낸다.

이러한 공격의 성공을 위해 필요한 평문의 수를 살펴보자. 이 공격에 사용된 차분 특성의 확률은 2^{-120}이고 필터링 과정을 통과할 확률은 2^{-96}이므로 $S/N = \frac{2^{32}\cdot 2^{-120}}{2^{-96}} \gg 1$이 된다. 따라서, 7-라운드 차분 특성을 만족하는 올바른 암호문 쌍 3개 정도면 키를 거의 유일하게 결정할 수 있다. 그러므로 필요한 평문 수는 $3\cdot 2^{121}$이면 충분하다.

위와 같은 방법으로 3장에서 구한 TYPE2의 특성식을 이용하면 8-라운드 키 SK_2과 SK_4를 찾을 수 있다. 마찬가지로 이때 필요한 평문의 수는 $3\cdot 2^{121}$이다. 따라서 8-라운드의 키 중 64-비트 SK_1, SK_2, SK_3, SK_4을 찾는 데에는 총 $3\cdot 2^{122}$평문이 필요하다. 이는 전수 조사 방법보다 효과적인 공격법이다.

V. 결론

본 논문에서는 PACA의 라운드 함수의 취약성을 이용하여 $3\cdot 2^{122}$개의 선택 평문을 이용하여 8-라운드 PACA에 대한 차분 공격법을 소개하였다. Feistel 구조를 가진 블록암호 알고리즘 PACA는 그 라운드 함수 F가 비교적 좋은 연산과 큰 S-박스를 쉬이서 사용함에도 불구하고 기본적인 8-라운드까지 공격이 되었다. 이러한 라운드 함수의 취약성을 이용하여 차분 분석 이외의 공격법들을 적용하여 볼 수 있을 것이다. 또한, 본 논문에서는 다루지 않았지만 차분 분석을 발전시킨 개념인 불능 차분 분석법과 부정 차분 분석법을 적용하면 더 나은 결과가 있을 것으로 추측된다.

본 논문은 라운드 함수 설계 시 암호학적으로 안전한 연산과 안전한 S-박스를 이용하여 설계하더라도 그러한 연산들을 어떻게 결합하느냐에 따라 안전성에 커다란 영향을 미칠 수 있다는 것을 단적으로 보여주고 있다.

참고문헌

[1] I. Ben-Aroya and E. Biham, "Differential Cryptanalysis of Lucipher," *Journal of Cryptology*, Vol. 9, No. 1, pp. 21 - 34, 1996.

[2] E. Biham, A. Biyukov, and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials," *Advances in Cryptology - EUROCRYPT'99*, LNCS 1592, pp. 12 - 23, Springer-Verlag, 1999.

[3] E. Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystem," *Journal of Cryptology*, Vol. 4, No. 1, pp. 3 - 72, 1991.

[4] L. R. Knudsen, "Truncated and Higer Order Differentials," *Fast Software Encryption- Second International Workshop*, LNCS 1008, pp. 196 - 211, Springer-Verlag, 1995.

[5] T. Jakobsen and L. R. Knudsen, "The Interpolation Attack on Block Ciphers," *Fast Software Encryption'97*, LNCS 1267, pp. 28 - 40, Springer-Verlag, 1995.

[6] National Instititude of Standards and Technology, "FIPS 197 : Advanced Encryption Standard," *Federal Information Processing Standard*, FIPS 197, 2001,

[7] D. Wagner, "The Boomerang Attack," *Fast Software Encryption'99*, LNCS 1636, pp. 156 - 170, Springer-Verlag, 1999.

[8] 김원준, 장성구, "*블록암호 알고리즘 PACA*," 대한민국특허청, 등록특허 10-0296958, 1998.

[9] 한국정보보호진흥원, "128비트 블록암호 알고리즘 표준 SEED," 정보통신단체표준, TTA. KO-12.0004, 1999.

[10] 정부전산정보관리소, "정부 전자서명 인증정책(GCA Certificate Policy)," 2000.