情報保護學會論文誌
第12券 第4號, 2002. 8

XTEA와 TEA의 축소된 라운드에 대한 불능 차분 공격

문 덕 재*, 황 경 덕**, 이 원 일*, 이 상 진*, 임 종 인*

Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA

Dukjae Moon*, Kyungdeok Hwang**, Wonil Lee*, Sangjin Lee*, Jongin Lim*

요 약

본 논문에서는 XTEA[7]와 TEA[6]의 축소된 라운드에 대한 불능 차분 공격 (Impossible Differential Cryptanalysis)에 관하여 알아본다. 이 두 블록 암호의 주요 설계원리는 단순성과 효율성의 추구이다. 그러나 단순성 추구가 큰 확산 (diffusion) 효과를 주지 못하여, XTEA와 TEA의 축소된 라운드에 대한 불능 차분 공격을 가능하게 한다. 구체적으로 말하면 12라운드 불능 차분 특성을 이용하여 14라운드 XTEA에 대하여 $2^{62.5}$개의 선택평문들과 2^{85}번의 암호화 과정을 통하여 128비트 마스터키를 찾아낼 수 있다. 또한, TEA의 경우 10라운드 불능 차분 특성을 이용하여 11라운드 마스터키를 $2^{52.5}$개의 선택평문들과 약 2^{84}번의 암호화 과정을 통하여 찾아낸다.

ABSTRACT

We present the impossible differential cryptanalysis of the block cipher XTEA[7] and TEA[6]. The core of the design principle of these block ciphers is an easy implementation and a simplicity. But this simplicity dose not offer a large diffusion property. Our impossible differential cryptanalysis of reduced-round versions of XTEA and TEA is based on this fact. We will show how to construct a 12-round impossible characteristic of XTEA. We can then derive 128-bit user key of the 14-round XTEA with $2^{62.5}$ chosen plaintexts and 2^{85} encryption times using the 12-round impossible characteristic. In addition, we will show how to construct a 10-round impossible characteristic of TEA. Then we can derive 128-bit user key of the 11-round TEA with $2^{52.5}$ chosen plaintexts and 2^{84}encryption times using the 10-round impossible characteristic.

Keyword : *XTEA and TEA, Impossible Differential Cryptanalysis, Impossible Characteristic*

Ⅰ. 서 론

1990년, E. Biham과 A. Shamir는 차분 공격 (Differential Cryptanalysis)[1]을 소개했다. 그 이후, 이 방법은 기존의 블록 암호들을 공격하는 매우 효과적인 것으로 받아들여졌다. 이러한 이유로 1990년대 중반 이후 등장한 블록 암호들은 설계할 때 반드시 차분 공격에 대한 안전성을 고려하게 되었다. 또한 차분 공격은 부정 차분 공격(Truncated Differential Cryptanalysis)[4], 고계 차분 공격(Higher Order Differential Cryptanalysis)[5], 불능 차분 공격 (Impossible Differential Cryptanalysis)[3] 등으로 변형되어 여러 블록 암호 알고리즘 공격에 사용되었다.

불능 차분 공격(Impossible Differential Cryptanalysis)[3]은 E. Biham, A. Biryukov, A. Shamir등에 의해 1998년 처음 소개되었다. 이 공격법은 선택 평문 공격으로 31라운드 Skipjack을

* 고려대학교 정보보호기술연구센터(CIST)({djmoon, wonil, sangjin, jilim}@cist.korea.ac.kr)
** 안철수 연구소(kdhwang@ahnlab.com)

분석하는데 사용되었다. 전형적인 차분 공격은 높은 확률의 차분 특성을 이용하여 키를 찾아내지만, 불능 차분 공격은 전혀 일어날 수 없는 차분 특성을 이용하여 키를 찾아낸다.

일반적인 불능 차분 공격은 다음과 같다. 우선, 불능 차분 특성을 찾아내고, 이 특성의 입력 차분을 만족하는 선택 평문 쌍에 대한 암호문 쌍을 얻는다. 이때, 미리 얻어진 차분 특성에서부터 유도되는 성질을 암호문 쌍의 차분이 만족하는지를 검사하여 만족하는 쌍만을 남기고, 일반적으로 마지막 한 라운드나 두 라운드의 키를 가정하여 남은 쌍을 복호화하여 불능 차분 특성의 출력 차분을 만족하는지 검사한다. 그 결과, 조건을 만족하는 라운드키는 버리고, 이 과정을 반복하여 최종적으로 남은 키를 올바른 키로 택한다.

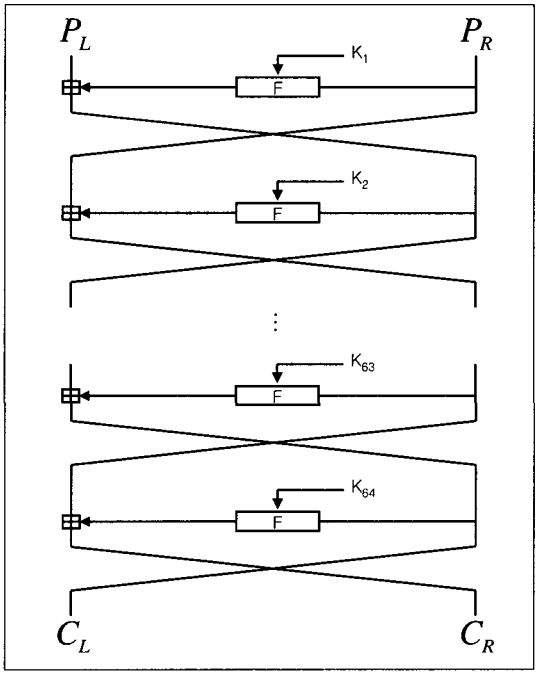
이 논문에서는, 12라운드 불능 차분 특성을 이용하여 14라운드 XTEA에 대한 불능 차분 공격을 제시한다. 이 공격에는 $2^{62.5}$개의 선택 평문들과 2^{85}번의 암호화 과정을 통하여 128비트의 마스터키를 찾아낸다. 또한, 11라운드 TEA는 10라운드 불능 차분 특성을 이용하여 $2^{52.5}$개의 선택 평문들 그리고 2^{84}번의 암호화 과정을 통하여 128비트의 마스터키를 찾아낸다.

II. TEA와 XTEA 소개

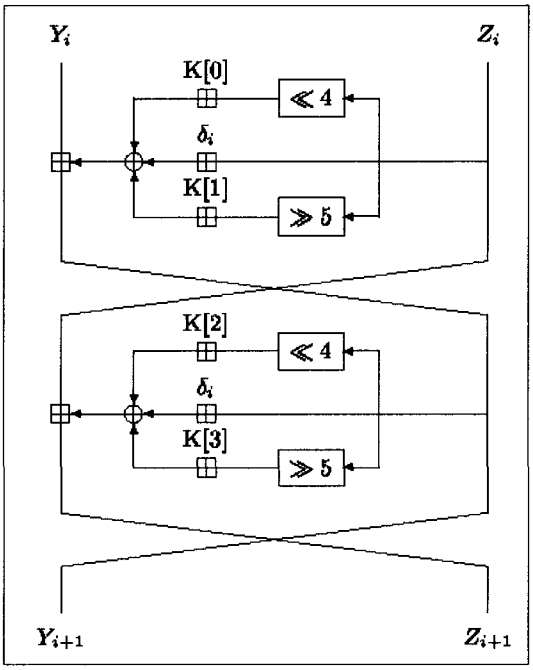
TEA(Tiny Encryption Algorithm)[6]는 David J. Wheeler와 R. Needham에 의해서 소개되었다. TEA는 안전한 암호화와 여러 시스템에 효과적으로 사용되어 질 수 있도록 만들어졌다. 이 암호는 간단한 키스케줄을 사용하는데, 이 간단한 스케줄로 인해 연관키 공격[8]이 가능하였다. 설계자들은 이런 약점들을 보완하여 XTEA(TEA Extensions)[7]를 다시 제안하였다.

2.1 TEA 알고리즘

TEA는 [그림 1]에서 보는 것과 같이 64비트 입력에 64라운드 (32싸이클[1]))를 반복하는 블록 암호이다. 각 라운드당 사용되는 라운드 함수 F는 2^{32}을 법으로 하는 덧셈(+), XOR(⊕) 그리고 좌우 쉬프트(≪,≫) 연산들로 구성된다. 이를 좀더 자세히 보면, i번째 싸이클의 입력 64비트 (Y_i, Z_i)에 대하여 출력 64비트 (Y_{i+1}, Z_{i+1})는 다음과 같고 [그림 2]에 잘 그려져 있다.



[그림 1] XTEA와 TEA의 구조



[그림 2] TEA의 i 번째 싸이클(cycle)

1) 키 스케줄이 반복되는 두라운드를 한 싸이클로 봄.

$$Y_{i+1} = Y_i + F(Z_i, K[0,1], \delta_i),$$
$$Z_{i+1} = Z_i + F(Y_{i+1}, K[2,3], \delta_i),$$
$$\delta_i = i \cdot \delta.$$

여기서 라운드함수 F는

$$F(X, K[j,k], \delta_i)$$
$$= ((X \ll 4) + K[j]) \oplus (X + \delta_i) \oplus ((X \gg 5) + K[k])$$

로 정의된다. 라운드함수에 사용되는 상수 $\delta(=\delta_0)$는 황금수로부터 유도된 16진수 "9E3779B9"이다.

이 알고리즘의 키스케줄은 매우 간단하다. 128비트의 마스터키 K를 (K[0],K[1],K[2],K[3])과 같이 네개의 32비트 블록으로 분할한다. 그 후 이 네개의 블록을 다음과 같은 방식으로 묶어 라운드키 (K_r)를 생성한다.

$$K_r = \begin{cases} (K[0], K[1]) & \text{if } r: \text{홀수} \\ (K[2], K[3]) & \text{if } r: \text{짝수} \end{cases},$$

여기서 r은 1부터 64까지의 자연수를 갖는다.

2.2 XTEA 알고리즘

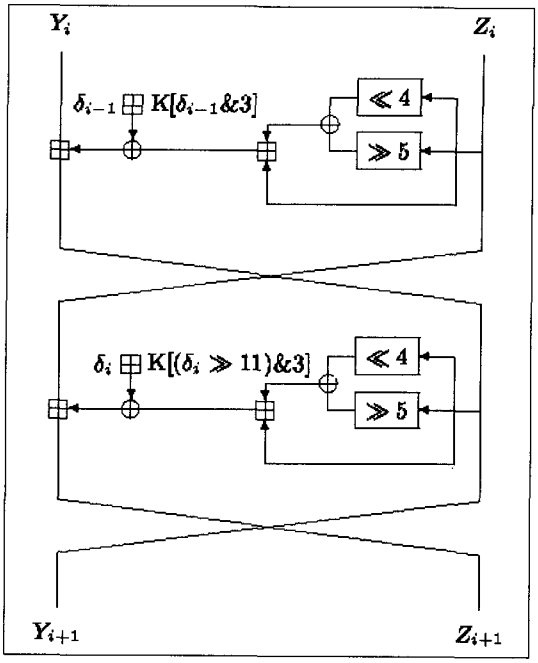
XTEA[7]는 TEA의 발전된 알고리즘이다. 따라서, XTEA는 TEA와 마찬가지로 기본적인 산술 및 논리 연산들을 사용하여 만들었다. 그러나 XTEA만의 특징은 δ_i의 끝의 두 비트 정보와 오른쪽으로의 열한번 쉬프트를 이용하여 키스케줄의 비정규성을 가미했다는 것이다. 이를 구체적으로 보면, i 번째 싸이클의 입력 64비트 (Y_i, Z_i)에 대하여 출력 64비트 (Y_{i+1}, Z_{i+1})는 다음과 같고 [그림 3]에서 잘 볼 수 있다.

$$Y_{i+1} = Y_i + F(Z_i, K_{2i-1}, \delta_{i-1}),$$
$$Z_{i+1} = Z_i + F(Y_{i+1}, K_{2i}, \delta_i),$$
$$\delta_i = i \cdot \delta.$$

여기서 라운드함수 F는

$$F(X, K_*, \delta_{**})$$
$$= \{((X \ll 4) \oplus (X \gg 5)) + X\} \oplus \{\delta_{**} + K_*\}$$

같이 정의 된다.



[그림 3] XTEA의 i 번째 싸이클(cycle)

라운드키는 TEA와 마찬가지로 마스터키를 분할하고 다음의 스케줄을 따라 생성한다.

$$K_r = \begin{cases} K[\delta_{\frac{r-1}{2}} \,\&\, 3] & \text{if } r: \text{홀수} \\ K[(\delta_{\frac{r}{2}} \gg 11) \,\&\, 3] & \text{if } r: \text{짝수} \end{cases}$$

여기서 r은 1부터 64까지의 자연수를 갖는다.

Ⅲ. 불능 차분 특성 구성

이 절에서는 XTEA에 대한 12라운드 불능 차분 특성과 TEA에 대한 10라운드 불능 차분 특성을 구성한다. XTEA와 TEA의 라운드 함수가 단지 한방향(왼쪽)으로의 확산(diffusion)을 갖는 비선형부분으로 덧셈연산을 사용하는 것과 자체 구조의 성질을 이용하여 불능 차분 특성을 구성할 수 있다. 구성되는 차분의 모양을 나타내기 위해 다음의 표기를 사용한다. α_i는 임의의 한 비트를 나타낸다. 여기서 i는 자연수이고 α는 영문 소문자를 나타낸다. 또한, Λ_x는 임의의 4비트를 나타내고, Λ는 영문 대문자를 나타낸다.

3.1 XTEA의 12라운드 불능 차분 특성

XTEA의 12라운드 불능 차분 특성이 어떻게 구

성되는가를 보기로 하자. 입력되는 차분의 모양 중 0이 아닌 최하위 비트는 단지 5비트 우 쉬프트(≫) 연산에만 영향을 받아 라운드마다 5비트만큼 우측으로 이동된다. 이는 본 알고리즘의 라운드함수의 확산(diffusion)이 왼쪽 한 방향으로만 영향을 주기 때문이다. 즉, 비선형부분인 덧셈연산에서 발생하는 carry는 왼쪽 방향으로 영향을 주기 때문에 차분의 0이 아닌 최하위 비트에 대하여 그 위치가 변하지 않고, 우 쉬프트에 의해서만 자리 이동이 생기게 된다. 이와 같은 성질을 이용하여 불능 차분 특성을 찾는다. 부록에 수록된 [표 1]에서 보듯이 만약 입력 차분이 다음과 같다면

$$(A_x\ a_1a_210\ 0_x0_x0_x0_x0_x0_x \| b_1000\ 0_x0_x0_x0_x0_x0_x0_x) \quad (1)$$

6라운드 후의 출력 차분 모양은 반드시 다음과 같아야만 한다.

$$(N_xO_xP_xQ_xR_xS_xf_1f_2100_x \| T_xU_xV_xW_xX_xY_xZ_xg_1g_2g_31) \quad (2)$$

또한, 12라운드 출력 차분이 다음과 같다면

$$(a_1000\ 0_x0_x0_x0_x0_x0_x \| A_x\ b_1b_210\ 0_x0_x0_x0_x0_x) \quad (3)$$

6라운드 복호화 후의 차분 모양은 반드시 다음과 같아야 한다.

$$(T_xU_xV_xW_xX_xY_xZ_xg_1g_2g_31 \| N_xO_xP_xQ_xR_xS_xf_1f_2100_x) \quad (4)$$

이때, 위 두 차분 특성을 연결한다면, 즉, 입력 차분 모양이 식 (1)이고 12라운드 출력 차분 모양이 식 (3)이라면, 반드시 식 (2)와 식 (4) 모양이 같아야만 한다. 그러나 적어도 32번째 비트와 64번째 비트가 다르기 때문에 이런 차분 특성은 결코 있을 수 없다. 따라서, 이 특성이 바로 우리가 구하는 XTEA의 12라운드 불능 차분 특성이다.

3.2 TEA의 10라운드 불능 차분 특성

같은 차분 성질을 이용하여, 만약 입력 차분이

$$(A_xB_xa_1a_2a_310_x0_x0_x0_x0_x \| C_xb_1b_2000_x0_x0_x0_x0_x) \quad (5)$$

모양 이라면, 5라운드 후의 출력차분 모양은 반드시

$$(O_xP_xQ_xR_xS_xT_xe_1e_2100_x \| U_xV_xW_xX_xY_xZ_x\Gamma_xf_1f_2f_31) \quad (6)$$

이어야 한다. 한편, 10 라운드 출력 차분이

$$(A_xa_1a_2000_x0_x0_x0_x0_x0_x \| B_xC_xb_1b_2b_310_x0_x0_x0_x0_x) \quad (7)$$

와 같은 모양이라면 5라운드 복호화 후의 차분 모양은

$$(U_xV_xW_xX_xY_xZ_x\Gamma_xf_1f_2f_31 \| O_xP_xQ_xR_xS_xT_xe_1e_2100_x) \quad (8)$$

이어야만 한다. 이때 입력 차분 모양이 식 (5)이고 10라운드 출력 차분 모양이 식 (7)라면, 반드시 식 (6)과 식 (8) 모양이 같아야만 한다. 그러나 32번째 비트와 64번째 비트를 비교해 보면 모양이 다르므로 이와 같은 차분은 결코 일어날 수 없다. 바로 이 특성이 TEA에 대한 10라운드 불능 차분 특성이고, 좀더 자세한 모양은 부록의 [표 2]에 수록해 놓았다.

Ⅳ. 불능 차분 특성을 이용한 공격

이 절에서는 앞 절에서 구성한 불능 차분 특성을 이용하여 14라운드 XTEA와 11라운드 TEA를 분석한다. 14라운드 XTEA에 대한 분석은 12라운드 불능 차분 특성을 가지고 2R-attack[9]을 한다 [표 1]. 또한 11라운드 TEA에 대하여는 10라운드 불능 차분 특성을 이용한 1R-attack[9]을 한다[표 2].

4.1 14라운드 XTEA 공격

12라운드 불능 차분 특성을 이용하여 14라운드 XTEA의 마지막 두 라운드 키를 찾아내는 방법을 소개하겠다. 이 공격을 위해 다음의 차분을 만족하는 2^7개 평문들의 구조(Structure)들을 사용한다.

$$(A_xa_1a_210\ 0_x0_x0_x0_x0_x \| b_10000_x0_x0_x0_x0_x0_x) \quad (9)$$

이 구조들은 약 $2^{13}\left(\approx\binom{2^7}{2}\right)$개의 평문쌍을 구성한다. 따라서, 주어진 $2^{55.5}$개의 구조들은 $2^{62.5}$개의 평문들과 $2^{68.5}$개의 평문쌍들을 만들 수 있고, 이렇게 만들어진 평문쌍들에 대하여 14라운드 암호화 차분을 구

한다. 또한, 우리가 찾아낸 12라운드 불능 차분 특성의 12라운드 출력에 대하여 두 라운드 암호화과정을 붙여 14라운드 암호문 차분을 구한다. 이렇게 구하여진 차분의 모양은 다음과 같다.

$$(A_xB_xa_1a_2a_310_x0_x0_x0_x0_x \| C_xD_xE_xF_x10000_x0_x0_x) \quad (10)$$

그리고, 주어진 평문쌍에 대한 14라운드 암호화 차분의 모양이 위의 모양 식 (10)과 같은 쌍들을 모을 수 있다. 이때, 한 암호문쌍이 위의 조건을 만족하려면 고정된 차분 비트(37비트)의 모양이 같아야 한다. 이렇게 만족할 확률은 $(2^{-4})^9 \times 2^{-1} \approx 2^{-37}$이다. 그러므로 위 과정을 통하여 남겨질 수 있는 암호문쌍의 수는 약 $2^{31.5}$개 ($= 2^{68.5} \times 2^{-37}$)이다. 남겨진 쌍들에 대하여 마지막 두 라운드의 가능한 2^{64}개의 키들을 가지고 두 라운드 복호화를 하고 만일 그 출력 차분이 12라운드 불능 차분 특성의 출력 차분과 일치하면 복호화에 사용된 키들은 키공간에서 제거한다. 즉, 14라운드 키에 대하여 한 라운드를 복호화하여 만든 13라운드 차분 중 불능 차분으로부터 유도된 13라운드의 좌측 32비트 모양과 같은지를 체크하고[2], 다시 13라운드의 키에 대하여 한 라운드를 복호화하여 만든 12라운드 차분 모양이 불능 차분의 12라운드 좌측 32비트의 모양과 같은지를 체크[3]하여 같다면 그 라운드키를 제거한다. 이때 13라운드의 좌측 32비트 모양 중 고정된 비트의 수는 26비트이고 12라운드의 경우는 31비트이므로 이 비트모양과 같은지 체크하여 같다면 라운드키를 제거한다. 따라서 한 암호문쌍에 대하여 복호화 키가 키공간에서 살아남을 확률은 $(1-2^{-26}) \times (1-2^{-31})$이다. 14라운드 출력 차분(6) 조건을 만족하여 남겨진 $2^{31.5}$개의 암호문쌍을 복호화한다면 마지막 두 라운드 키공간에 약 $2^{64} \times \{(1-2^{-26})(1-2^{-31})\}^{2^{31.5}} < 2^{-3.4}$개의 틀린 키 쌍(wrong key pair)이 남는다. 즉, 단지 한개의 올바른 키쌍 (K_{13}, K_{14})만이 남는다는 것을 의미한다.

위에서 설명한 공격 과정을 정리해 보면 다음과 같다.

<XTEA에 대한 불능차분공격>

목 표 : 13, 14라운드 키 쌍 (K_{13}, K_{14}) 찾기.

〔1〕 차분(9)를 만족하는 평문쌍을 $2^{55.5}$개의 구조들에서 $2^{68.5}$개 선택하고, 각각에 대응하는 14라운드 암호문쌍을 얻는다.

〔2〕 획득한 암호문쌍들의 차분 중 차분(10)을 만족하는 암호문쌍들을 모은다.

〔3〕 2〕 과정에서 모여진 암호문쌍들 중 임의의 쌍을 선택한다.

〔4〕 키 공간의 모든 키 쌍 (K_{13}, K_{14})에 대하여,

(a) 선택된 암호문쌍에 대하여 12라운드까지 복호화과정을 거친다.

(b) 복호화된 12라운드 출력쌍의 차분을 계산한다.

(c) 계산된 차분과 12라운드 불능 차분 특성의 12라운드 출력 차분을 비교한다. 만약 이 두 차분이 같다면, 복호화키 쌍을 키 공간 에서 제거한다.

〔5〕 만약 $|K_{13}| \le \varepsilon$ 이고, $|K_{14}| \le \varepsilon'$이라면, 위 과정을 끝마친다. 아니라면, 〔3〕 과정으로 이동하여 위 과정을 계속한다.(여기서 ε과 ε'은 작은 정수들이다.)

이 공격에 필요한 암호화 과정은 약 $2^{85} \approx 2^{64} \cdot 2^{-5} + 2^{64}\{(1-2^{-26})(1-2^{-31})\} \cdot 2^{-5} + \cdots + 2^{64}\{(1-2^{-26})(1-2^{-31})\}^{(2^{31.5}-1)} \cdot 2^{-5}$이고, 2^{-5}은 XTEA 암호화의 두 라운드 암호화를 의미한다. 위 식은 12라운드 불능 차분 특성에서 유도된 14라운드 출력 차분을 만족하는 $2^{31.5}$개의 암호문쌍을 가지고 13, 14라운드 키공간 2^{64}에 대하여 복호화 과정을 통해 올바르지 않은 키들을 제거하여 최종 올바른 키 한 쌍을 남기는 암호화 과정이다. 이때, 한 암호문쌍을 통해 키공간이 $(1-2^{-26}) \times (1-2^{-31})$ 만큼씩 줄어들고, 줄어든 키공간에 대하여 다른 암호문쌍을 통해 다른 올바르지 않은 키들을 제거하고, 이런 과정을 가지고 있는 암호문쌍에 대하여 계속하면 올바른 키만 남게된다. 위의 방법을 통하여 64비트의 마스터키를 찾고 나머지 64비트의 값들은 전수조사를 통하여 얻을 수 있다.

4.2 11라운드 TEA 공격

앞에서 설명한 방법과 같은 방법으로 11라운드 TEA에 대한 128비트 마스터키를 찾을 수 있다. 이 공격은 〔표 2〕의 10라운드 불능 차분 특성을 이용

2) 13라운드의 우측 32비트 모양은 14라운드의 좌측 32비트 모양과 동일하기 때문에 체크할 필요가 없다.

3) 12라운드의 우측 32비트 모양은 13라운드의 좌측 32비트 모양과 동일하기 때문에 체크할 필요가 없다.

한다. 그 과정을 살펴보면, 다음의 차분을 만족하는 2^{17}개의 평문들의 구조들을 얻는다.

$$(A_xB_xa_1a_2a_31\,0_x0_x0_x0_x0_x \| C_xb_1b_2000_x0_x0_x0_x0_x) \quad (11)$$

획득된 평문쌍들에 대응하는 11라운드 암호문에 대하여 다음 모양의 차분을 갖는 암호쌍들을 모은다.

$$(A_xB_xa_1a_2a_31\,0_x0_x0_x0_x0_x \| C_xD_xE_xF_x10000_x0_x0_x) \quad (12)$$

이때의 임의의 평문쌍이 위 암호문 차분을 만족할 확률은 $(2^{-4})^9 \times 2^{-1} \approx 2^{-37}$이고, 한 암호문쌍에 대하여 복호화 키가 키공간에서 살아남으려면 11라운드 키에 대하여 10라운드 좌측 32비트의 모양과 일치해야 하므로 그 확률은 $1-2^{-26}$이다. 올바른 키를 찾기 위해 필요한 평문쌍의 수를 N이라 놓으면 N은 $2^{64}\times(1-2^{-26})^N < 1$을 만족해야 한다. 따라서, N은 약 $2^{31.5}$이다. 결과적으로 총 필요한 선택 평문쌍의 수는 $2^{37}\times 2^{31.5}=2^{68.5}$개이다. 이 쌍들을 구조들을 이용하여 얻는다면 한 구조당 2^{33}개의 쌍을 얻을 수 있고 $2^{35.5}$개의 구조들을 사용한다면 $2^{35.5}\times 2^{17}=2^{52.5}$개의 선택평문만 필요하게 된다. 이렇게 얻어진 평문쌍을 가지고 64비트의 11라운드 키(K_{11})를 찾는다. 이 공격을 요약하면 다음과 같다.

목 표 : 11라운드 키(K_{11}) 찾기

[1] 차분(11)을 만족하는 평문쌍을 $2^{35.5}$개의 구조들 에서 $2^{68.5}$개 선택하고, 각각에 대응하는 11라운드 암호문쌍을 얻는다.
[2] 획득한 암호문쌍들의 차분 중 차분(12)을 만족하 는 암호문쌍들을 모은다.
[3] [2] 과정에서 모여진 암호문쌍들 중 임의의 쌍을 선택한다.
[4] 키 공간의 모든 키(K_{11})에 대하여,
(a) 선택된 암호문쌍에 대하여 10라운드까지 복 호화과정을 거친다.
(b) 복호화된 10라운드 출력쌍의 차분을 계산한다.
(c) 계산된 차분과 10라운드 불능 차분 특성의 10 라운드 출력 차분을 비교한다. 만약 이 두 차분이 같다면, 복호화키 쌍을 키 공간 에서 제거한다.
[5] 만약 $|K_{11}| \le \epsilon$이라면, 위 과정을 끝마친다. 아니라면, [3] 과정으로 이동하여 위 과정을 계속한 다. (여기서 ϵ은 작은 정수이다.)

이 공격에 필요한 암호화 과정은 약 $2^{84} \approx 2^{64}\cdot 2^{-6} + 2^{64}(1-2^{-26})\cdot 2^{-6} + \cdots + 2^{64}(1-2^{-26})^{2^{31.5}-1}\cdot 2^{-6}$ 이고, 2^{-6}은 TEA 암호화의 한 라운드 암호화를 의미한다. 위의 방법을 통하여 64비트의 마스터키를 찾고 나머지 64비트의 값들은 전수조사를 통하여 얻을 수 있다.

V. 결 론

지금까지 본 논문에서는 XTEA와 TEA의 알고리즘을 소개하고, 알고리즘의 구조적 특성을 이용하여 XTEA에 대한 12라운드 불능 차분 특성과 TEA에 대한 10라운드 불능 차분 특성을 찾았다. 이렇게 찾은 XTEA의 12라운드 불능 차분 특성과 $2^{62.5}$개의 선택평문을 이용하여 14라운드 XTEA의 마스터키를 찾을 수 있다. 이때 사용되는 암호화 과정은 2^{85}이다. TEA 경우, 10라운드 불능 차분 특성과 $2^{52.5}$개의 선택평문을 이용하여 11라운드 TEA의 마스터키를 찾을 수 있다. 이 공격의 암호화 과정은 2^{84}이다.

참 고 문 헌

[1] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like cryptosystems", *Advances in Cryptology - CRYPTO'90*, LNCS 537, Springer-Verlag, 1991, pp. 2~21.
[2] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys", *Advances in Cryptology - EUROCRYT'93*, LNCS 765, Springer-Verlag, 1994, pp. 398~409.
[3] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of skipjack reduced to 31 round using impossible differentiala", *Advances inCryptology - EUROCRYT'99*, LNCS 1592, Springer-Verlag, 1999, pp. 12~23.
[4] L. R. Knudsen, "Truncated and Higher Order Differential", *Fast Software Encrytion Workshop 94*, LNCS 1008, Springer-Verlag, 1995, pp. 229~236.
[5] S. Moriai, T. Shimoyama and T. Kaneko, "Higher Order Differential Attack of a CAST cipher", *Fast Software Encrytion Workshop 98*, LNCS 1372, Springer-Verlag,

1998, pp. 17~31.

[6] D. Wheeler and R. Needham, "TEA, a TinyEncryption Algorithm", *Fast Software Encryption*, Second International Workshop Proceedings, Springer-Verlag, 1995, pp. 97~110.

[7] D. Wheeler and R. Needham, "TEA Extensions", October 1997. Available at http://www.cl.cam.ac.uk/ftp/users/djw3/xtea.ps.

[8] J. Kelsey, B. Schneier and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", *In Information and Communications Security-Proceedings of ICICS 1997, Lecture Notes in Computer Science 1334*, Springer-Verlag, 1997.

[9] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer-Verlag, 1993.

[부 록]

[표 1] XTEA의 12라운드 불능 차분 특성

라운드수	왼쪽 차분	오른쪽 차분
0 (입력)	$A_x\ a_1a_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$b_1000\ 0_x\ 0_x0_x\ 0_x0_x\ 0_x0_x$
1	$b_1000\ 0_x\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$B_x\ c_1c_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$
2	$B_x\ c_1c_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$C_xD_x\ d_1d_2d_31\ 0_x\ 0_x0_x\ 0_x0_x$
3	$C_xD_x\ d_1d_2d_31\ 0_x\ 0_x0_x\ 0_x0_x$	$E_xF_x\ G_xH_x\ 1000\ 0_x\ 0_x0_x$
4	$E_xF_x\ G_xH_x\ 1000\ 0_x\ 0_x0_x$	$I_xJ_x\ K_xL_x\ M_x\ e_1100\ 0_x0_x$
5	$I_xJ_x\ K_xL_x\ M_x\ e_1100\ 0_x0_x$	$N_xO_x\ P_xQ_x\ R_xS_x\ f_1f_210\ 0_x$
6	$N_xO_x\ P_xQ_x\ R_xS_x\ f_1f_210\ 0_x$	$T_xU_x\ V_xW_x\ X_xY_x\ Z_x\ g_1g_2g_31$
6	$T_xU_x\ V_xW_x\ X_xY_x\ Z_x\ g_1g_2g_31$	$N_xO_x\ P_xQ_x\ R_xS_x\ f_1f_210\ 0_x$
7	$N_xO_x\ P_xQ_x\ R_xS_x\ f_1f_210\ 0_x$	$I_xJ_x\ K_xL_x\ M_x\ e_1100\ 0_x0_x$
8	$I_xJ_x\ K_xL_x\ M_x\ e_1100\ 0_x0_x$	$E_xF_x\ G_xH_x\ 1000\ 0_x\ 0_x0_x$
9	$E_xF_x\ G_xH_x\ 1000\ 0_x\ 0_x0_x$	$C_xD_x\ d_1d_2d_31\ 0_x\ 0_x0_x\ 0_x0_x$
10	$C_xD_x\ d_1d_2d_31\ 0_x\ 0_x0_x\ 0_x0_x$	$B_x\ c_1c_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$
11	$B_x\ c_1c_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$a_1000\ 0_x\ 0_x0_x\ 0_x0_x\ 0_x0_x$
12 (출력)	$a_1000\ 0_x\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$A_x\ b_1b_210\ 0_x0_x\ 0_x0_x\ 0_x0_x$

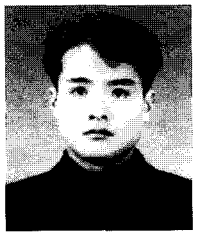
[표 2] TEA의 10 라운드 불능 차분 특성

라운드수	왼쪽 차분	오른쪽 차분
0 (입력)	$A_xB_x\ a_1a_2a_31\ 0_x\ 0_x0_x\ 0_x0_x$	$C_x\ b_1b_200\ 0_x0_x\ 0_x0_x\ 0_x0_x$
1	$C_x\ b_1b_200\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$D_xE_x\ c_1c_2c_31\ 0_x\ 0_x0_x\ 0_x0_x$
2	$D_xE_x\ c_1c_2c_31\ 0_x\ 0_x0_x\ 0_x0_x$	$F_xG_x\ H_xI_x\ 1000\ 0_x\ 0_x0_x$
3	$F_xG_x\ H_xI_x\ 1000\ 0_x\ 0_x0_x$	$J_xK_x\ L_xM_x\ N_x\ d_1100\ 0_x0_x$
4	$J_xK_x\ L_xM_x\ N_x\ d_1100\ 0_x0_x$	$O_xP_x\ Q_xR_x\ S_xT_x\ e_1e_210\ 0_x$
5	$O_xP_x\ Q_xR_x\ S_xT_x\ e_1e_210\ 0_x$	$U_xV_x\ W_xX_x\ Y_xZ_x\ \Gamma_x\ f_1f_2f_31$
5	$U_xV_x\ W_xX_x\ Y_xZ_x\ \Gamma_x\ f_1f_2f_31$	$O_xP_x\ Q_xR_x\ S_xT_x\ e_1e_210\ 0_x$
6	$O_xP_x\ Q_xR_x\ S_xT_x\ e_1e_210\ 0_x$	$J_xK_x\ L_xM_x\ N_x\ d_1100\ 0_x0_x$
7	$J_xK_x\ L_xM_x\ N_x\ d_1100\ 0_x0_x$	$F_xG_x\ H_xI_x\ 1000\ 0_x\ 0_x0_x$
8	$F_xG_x\ H_xI_x\ 1000\ 0_x\ 0_x0_x$	$D_xE_x\ c_1c_2c_31\ 0_x\ 0_x0_x\ 0_x0_x$
9	$D_xE_x\ c_1c_2c_31\ 0_x\ 0_x0_x\ 0_x0_x$	$A_x\ a_1a_200\ 0_x0_x\ 0_x0_x\ 0_x0_x$
10 (출력)	$A_x\ a_1a_200\ 0_x0_x\ 0_x0_x\ 0_x0_x$	$B_xC_x\ b_1b_2b_31\ 0_x\ 0_x0_x\ 0_x0_x$

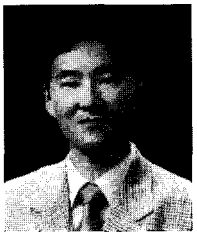
〈著者紹介〉

문 덕 재 (Duk-Jae Moon)
2000년 2월 : 서울시립대학교 수학과 학사
2001년 3월~현재 : 고려대학교 정보보호대학원 석사 과정
〈관심분야〉 블록 암호 및 스트림 암호 분석

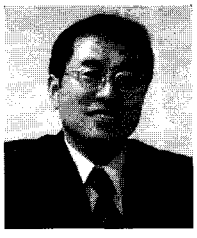
황 경 덕 (Kyung-Deok Hwang)
2000년 2월 : 고려대학교 수학과 학사
2002년 2월 : 고려대학교 수학과 석사
2002년 2월~현재 : 안철수 연구소 연구원
〈관심분야〉 블록 암호 및 스트림 암호 분석 및 설계



이 원 일 (Won-Il Lee)
1998년 2월 : 고려대학교 수학과 학사
2000년 2월 : 고려대학교 수학과 석사
2000년 3월~현재 : 고려대학교 수학과 박사과정
〈관심분야〉 블록 암호 및 스트림 암호 분석 및 설계



이 상 진 (Sang-Jin Lee) 정회원
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 8월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구소 선임 연구원
1999년 3월~현재 : 고려대학교 자연과학대학 부교수, 고려대학교 정보보호대학원 겸임교수, 고려대학교 정보보호기술연구센터 연구실장
〈관심분야〉 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석



임 종 인 (Jong-In Lim) 정회원
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국통신정보보호학회 편집위원장, 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 분석