XTEA의 연관키를 이용한 차분 공격

고영대,이원일,홍석희,이태건,이상진

고려대학교 정보보호대학원 정보보호연구센터

Related Key Differential Cryptanalysis of XTEA

Young-dai Ko, Won-il Lee, Seok-hie Hong, Tae-geon Lee, Sang-jin Lee

Center for Information of Security of Technologies, Korea University

요 약

이 논문에서는 블록 암호 알고리즘인 *XTEA*에 관한 연관키를 이용한 차분공격에 대하여 설명한다. 이 것은 *XTEA* 알고리즘이 *TEA*가 갖고 있는 취약한 키 스케줄을 보완하여 *Kelsey* 등이 제안한 연관키 공격에 대응하기 위하여 설계 되었지만, *26* 라운드로 줄인 *XTEA* 또한 우리의 연관키를 이용한 차분공격에 안전하지 못하다는 것을 보여준다. 또한 키 스케줄에 의하여 다양하게 변화된 라운드의 XTEA에 관한 연관키 공격이 가능하다. 이 때 필요한 선택평문과 암호화 과정은 각각 $2^{18.5}$과 $2^{115.21}$이다.

I. 서론

1. 개 요

1997년에 *Kelsey* 등은 *TEA* (*Tiny Encryption Algorithm*) [6]의 단순한 키 스케줄을 이용하여 전체 *64* 라운드에 대한 연관키 공격 [3]을 하였다. 그래서 *TEA*의 설계자들은 이러한 연관키 공격에 대응하기 위하여 키 스케줄을 변경하고 라운드 함수에도 약간의 변화를 주어 *XTEA* (*Extend TEA*) [7]를 만들었다. *XTEA*는 *TEA*와 마찬가지로 덧셈, *XOR* 그리고 순환이동 등의 간단한 연산만으로 이루어진 라운드 함수를 사용한 *64* 라운드 블록암호이다. *XTEA*의 키 스케줄은 *TEA*와는 달리 불규칙적으로 이루어져 있다. 이러한 불규칙성으로 인하여 *TEA*에 적용되었던 연관키 공격에 대해 *XTEA*는 안전할 수 있었다. 그러나, 우리가 사용한 연관키를 이용한 차분 공격은 *26* 라운드로 줄인 *XTEA*에 적용할 수 있고, 이때 필요한 선택평문과 연산량은 각각 $2^{18.5}$ 과 $2^{115.21}$ 이다.

연관키 공격은 *E. Biham*이 *LOKI*를 공격 [5]하면서 처음 제안한 개념으로 *LOKI*의 키 스케줄이 마스터 키의 순환이동만으로 이루어져 있다는 특성을 이용한 일종의 *Slide* 공격 방법 [8]이다. 이러한 연관키 개념을 이용하여 키 스케줄이 취약한 알고리즘에 대해서 *Kelsey* 등은 1996년도에 *IDEA, G-DES, GOST, SAFER* 와 *Triple-DES*를 분석 [1]하였고, 다음해인 1997년에는 *3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2* 그리고 *TEA*에 관한 연관키 공격을 제시 [3]하였다. 또, 가장 최근에는 G. Jakimoski 등이 연관키를 이용한 불능 차분공격으로 *AES-192* 에 대한 *8* 라운드 공격을 하였다.

현재까지 연관키 공격을 포함하여 *TEA*와 *XTEA* 알고리즘에 대한 분석은 그다지 많지 않다 (표 1참조). 문덕재 등이 *FSE'02*에서 불능 차분을 이용하여 *12* 라운드 *TEA*와 *14* 라운드 *XTEA*에 대한 공격 [4]을 하였고, 올해 *ICISC'03*에서 홍득조 등이 차분특성을 이용한 *15* 라운드 *XTEA*에 대해서, 그리고 부정차분특성을 이용하여 *17* 라운드 *TEA*와 *23* 라운드 *XTEA* 에 대한 공격 ([2])을 제시하였다. 이 논문에서는 홍득조 등이 사용한 부정차분 특성을 이용한 *26* 라운드 *XTEA*에 관한 연관키 공격에 대해서 설명할 것이다. 따라

서, 이 논문의 대부분의 표기법 또한 [2]를 따를 것이다.

표 1: *TEA*와 *XTEA*에 관한 다양한 공격결과.

구 분	공격방법	라운드	선택평문	복잡도
TEA	연관키[3]	*64*	2^{34}	2^{34}
	불능차분[4]	*12*	$2^{52.5}$	2^{84}
	부정차분[2]	*17*	*1920*	$2^{123.37}$
XTEA	불능차분[4]	*14*	$2^{62.5}$	2^{85}
	부정차분[2]	*23*	$2^{20.55}$	$2^{120.65}$
본 논문	연관키	*26*	$2^{18.5}$	$2^{115.21}$

이 논문의 본문에서는 우선 *XTEA* 블록암호에 대해서 간략하게 소개하고 홍득조 등이 사용한 *8* 라운드 부정차분 특성을 설명한다. 그 다음에 이 논문의 핵심인 연관키 개념을 이용한 *26* 라운드 *XTEA*에 차분공격에 대해서 언급한다.

II. 본문

1. *XTEA* 알고리즘

*XTEA*는 *64*-bit 블록과 *128*-bit 비밀키를 사용하는 64 라운드 *Feistel* 구조로 이루어진 알고리즘이다. *128*-bit 비밀키 *K*는 네 개의 *32*-bit 워드 *K[0], K[1], K[2], K[4]*로 나뉘어진 후 키 스케줄에 따라 각각의 라운드에 사용된다. 라운드 상수 δ=*0x9e3779b9*를 사용하는 라운드 함수 *F*는 아래와 같이 구성되어 진다. $1 \le n \le 64$인 n에 대해서,우선 (L_n, R_n)을 n번째 라운드의 입력값이라 하고 (L_{n+1}, R_{n+1})을 n번째 라운드의 출력값이라고 하면 $L_{n+1}=R_n$ 이고 R_{n+1}은 다음과 같이 계산된다. $1 \le i \le 32$ 인 i에 대해서 $n = 2i-1$ 이면,

$$R_{n+1} = L_n + ((R_n \ll 4 \oplus R_n \gg 5) + R_n) \oplus ((i-1)\cdot\delta \gg 11)\&3]),$$

n = 2i 이면,

$$R_{n+1} = L_n + ((R_n \ll 4 \oplus R_n \gg 5) + R_n) \oplus (i\cdot\delta + K[(i\cdot\delta \gg 11)\&3]).$$

여기서, +는 덧셈연산, ⊕는 비트별 *XOR* 연산, ·는 곱셈연산, &는 비트별 *AND* 연산을 나타낸다. 그림 1은 $n = 2i$일 때 *XTEA*의 라운드 함수를 표현한 것이다. *XTEA*는 *TEA*와는 달리 불규칙적인 키 스케줄을 갖는다. 아래의 표 2는 전체 *64* 라운드에 사용되는 부분키를 설명한 것이다.

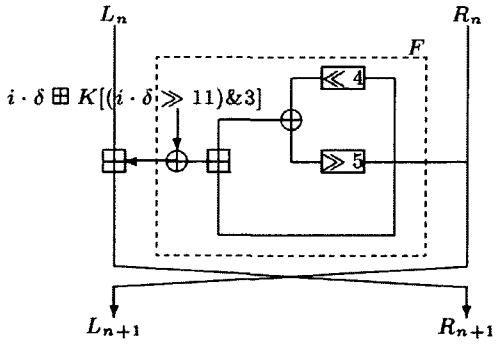

그림 1 *XTEA*의 라운드 ($n=2i$) 함수

표 2. *XTEA*의 키 스케줄

R	1	2	3	4	5	6	7	8
Key	K[0]	K[3]	K[1]	K[2]	K[2]	K[1]	K[3]	K[0]
R	9	10	11	12	13	14	15	16
Key	K[0]	K[0]	K[1]	K[3]	K[2]	K[2]	K[3]	K[1]
R	17	18	19	20	21	22	23	24
Key	K[0]	K[0]	K[1]	K[0]	K[2]	K[3]	K[3]	K[2]
R	25	26	27	28	29	30	31	32
Key	K[0]	K[1]	K[1]	K[1]	K[2]	K[0]	K[3]	K[3]
R	33	34	35	36	37	38	39	40
Key	K[0]	K[2]	K[1]	K[1]	K[2]	K[1]	K[3]	K[0]
R	41	42	43	44	45	46	47	48
Key	K[0]	K[3]	K[1]	K[2]	K[2]	K[1]	K[3]	K[1]
R	49	50	51	52	53	54	55	56
Key	K[0]	K[0]	K[1]	K[3]	K[2]	K[2]	K[3]	K[2]
R	57	58	59	60	61	62	63	64
Key	K[0]	K[1]	K[1]	K[0]	K[2]	K[3]	K[3]	K[2]

2. *XTEA*에 대한 부정차분 공격

[2]에서 홍득조 등은 *23* 라운드 *XTEA*에 대하여 부정차분 특성을 이용한 공격을 하였다. 이 절에서는 *XTEA*가 갖고 있는 그러한 부정차분 특성에 대하여 언급하기로 한다. 이러한 특성은 *XTEA*가 순환이동과 덧셈 등의 단순한 연산만을 사용하는 라운드 함수로 이루어져 있기 때문에 발생한다. 특히, mod 2^{32}의 덧셈연산에서 carry 비트는 하위 비트에는 영향을 끼치지 않는 성질 때문에 우리는 확률 *1*로써 *8* 라운드 부정차분 특성을 꾸밀 수 있다.

(1) *8* 라운드 부정차분 특성

라운드 함수의 입력차분이 오른쪽은 *0*이고, 왼쪽은 *30*번째 비트에서만 차분을 갖는 선택평문을

생각하면 확률 *1*을 갖는 *8* 라운드 부정차분 특성은 그림 2와 같이 구성된다. 그림에서 흰색 부분은 차분이 *0*인 부분이고, 검정색인 부분은 확률 *1*로써 차분이 *1*인 부분으로 우리가 주의깊게 관찰할 곳이다. 여기서 회색 부분은 *XTEA*의 부정차분 특성에서 전혀 고려되지 않는다. 위에서 잠깐 언급했듯이, 덧셈 연산에 의한 carry bit는 하위 bit에는 영향을 끼치지 않기 때문에 왼쪽 입력값의 *30*번째 차분 bit는 순환이동에 의하여 *8* 라운드 이후의 왼쪽 출력값의 *0*번째 bit로 이동하게 된다.

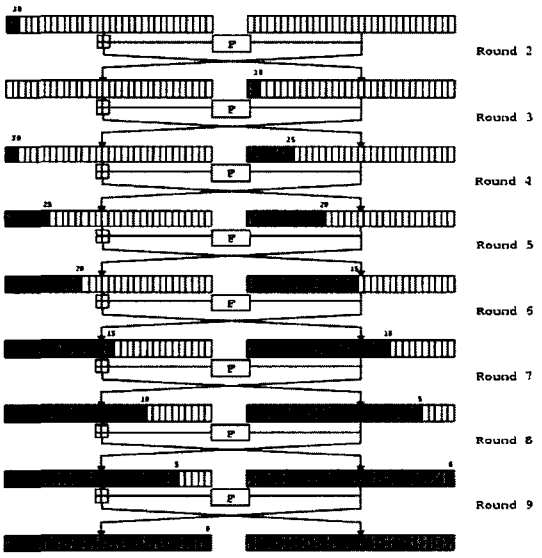

그림 2 XTEA의 8 라운드 부정차분 특성

(2) 공격 방법

1 라운드의 출력차분을 (1) 에서 언급한 8 라운드 부정차분 특성을 만족하도록 하기 위한 평문구조로 꾸민다면, 위의 특성식은 실제 *2* 라운드부터 *9* 라운드까지 적용될 수 있다. 평문구조에 대한 자세한 설명은 [2]를 참조한다. 그림 3은 암호문으로부터 검정색 부분을 계산하는 방법에 대하여 나타낸 것이다. 즉 검정색 부분을 계산하기 위해서는 점으로 찍힌 부분과 회색 부분의 값을 알아야만 한다. 예를 들어, *10* 라운드 왼쪽 출력값의 *0*번째와 *5*번째 bit의 차분값과 오른쪽 출력값의 *0*번째 차분값을 안다면 *10* 라운드의 왼쪽 입력차분의 검정색 부분을 계산할 수 있다. *11* 라운드에서는 왼쪽 출력차분의 *0*~*10*번째 bit, 오른쪽 출력차분의 *0*~*5*번째 bit 그리고 *K[0]*의 *0*~*4*번째 값을 알 수 있으면 *11* 라운드 입력차분의 회색부분을 계산할 수 있다 - 실제로는 *11* 라운드 왼쪽 차분의 *0*번째와 *5*번째 bit만 계산할 수 있다 -. 이러한 방법으로 라운드 함수의 부분키 bit들을 추측함으로써 일반적인 구조 (TEA의 경우)의 17 라운드까지 공격할 수 있다.

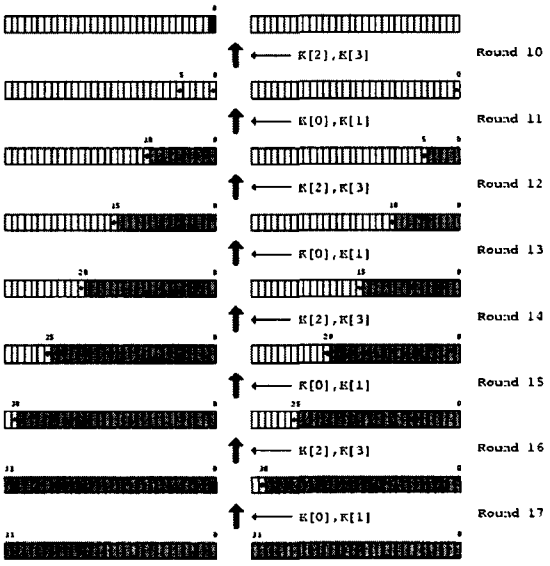

그림 3. 공격 방법

검정색 부분과 관련된 키 bit들은 매 라운드마다 *5*bit씩 증가한다. 그래서 *17* 라운드 이후의 암호문 쌍에 대하여 대응되는 라운드키를 추측하면 *10* 라운드 입력차분의 검정색 부분을 계산할 수 있다. 그런데, *TEA*와 달리 *XTEA*는 불규칙적인 키 스케줄을 갖는다. 표 3을 이용하면 특정한 부분키가 일정 라운드 동안은 사용되지 않는 것을 볼 수 있다. 예를 들어 *24* 라운드부터 *30* 라운드까지는 *K[3]*가 전혀 사용되지 않는다. 따라서, *9* 라운드부터 *30* 라운드의 변화된 *XTEA*를 생각한다면 이것은 위의 공격방법에 자연스럽게 *XTEA* *5* 라운드를 더 확장시킬 수 있음을 의미한다. 이러한 공격방법은 *121*-bit 비밀키를 복구하기 위해서 $2^{20.55}$개의 선택평문과 $2^{120.65}$의 암호화 과정을 요구한다.

3. 27 라운드 *XTEA*에 대한 연관키를 이용한 차분공격

여기서는 이 논문에서 제안하고 있는 *XTEA*의 연관키를 이용한 차분공격에 대하여 설명하고자 한다. 핵심 아이디어는 키 부분에 차분을 주고 그 차분을 라운드 함수의 입력차분을 이용하여 제거한 후 전체 공격하고자 하는 라운드를 늘리는 것이다. 그리고 다음 키 차분을 갖는 부분의 라운드는 2장에서 언급한 부정차분 특성을 이용하여 *8*

라운드 차분 특성식을 꾸민 후 위와 동일한 방법으로 공격한다.

우선, 두 개의 연관키 $K=(K[0], K[1], K[2], K[3])$ 와 $K'=(K[0]\oplus e_{30}, K[1], K[2], K[3])$ 그리고, K에 대응하는 평문 $P=(P_L,P_R)$ 과 K'에 대응하는 평문 $P=(P_L\oplus e_{30},P_R)$을 고려한다. 여기서 e_{30}은 30번째 비트만 1의 값을 갖고 나머지는 0의 값을 갖는 32-bit 워드를 의미한다. 즉, $K[0]$의 30번째 bit에서만 차분을 갖는 두개의 키에 대해서, 1 라운드의 왼쪽 입력 차분 또한 30번째 bit에서만 차분을 갖는 다음과 같은 1라운드 평문 구조 $S(P)$를 고려하면 1 라운드 이후의 출력 차분은 확률 0이 된다.

$$S(P)=\{P,P\oplus(e_{31},0),P\oplus(e_{30},0),P\oplus(e_{31}\oplus e_{30},0)\}$$

또한 XTEA의 키 스케줄에 의하면 2 라운드부터 7 라운드까지는 $K[0]$가 사용되지 않으므로 우리는 8 라운드까지 입력차분이 0인 특성식을 꾸밀 수 있다. 8 라운드의 키 차분에 의하여 왼쪽 출력은 30번째 bit가 1이 되기 때문에 우리는 2장에서 세운 부정차분 특성을 이용할 수 있고 이를 이용하여 25 라운드 XTEA의 대응되는 암호문과 $K[0], K[2], K[3]$의 각각 32-bit 씩 96-bit와 $K[1]$의 15 -bit를 추측하여 16 라운드 왼쪽 입력 차분이 1인지 만족하는지를 계산함으로써 비밀키 111-bit를 복구할 수 있다.

XTEA 키 스케줄의 특이성에 의하여 이 방법은 9 라운드부터 34 라운드 까지의 XTEA 26 라운드에 대한 공격을 가능하게 한다. 공격 방법은 2라운드 평문구조를 이용한다는 것과 연관키 $K=(K[0], K[1], K[2], K[3])$ 와 $K'=(K[0], K[1]\oplus e_{30}, K[2], K[3])$를 이용한다는 부분에서만 상이하다. 26라운드 공격에 사용하는 평문 구조 $S'(P)$는 다음과 같다.

$$S'(P)=\{P\}\cup\{P\oplus(w,v):w\in A,v\in X\}$$

여기서, X는 다음과 같다.

X={01000010···0, 01000110···0, 01001110···0,
01011110···0, 01111110···0, 00111110···0,
11000010···0, 11000110···0, 11001110···0,
11011110···0, 11111110···0, 10111110···0}

이러한 2라운드 평문구조를 이용하면 11라운드의 입력차분과 키 차분에 의하여 11라운드 출력차분이 (0, 0)이 된다. 16 라운드에서 다시 키 차분에 의한 암호문의 출력차분이 다시 발생하게 되는데 이 부분에서부터 부정차분 특성식을 꾸미게 되면 위와 동일한 방법으로 26라운드 XTEA에 대한 비밀키 116-bit를 성공확률 96.9%로 선택평문 $(121/4\times12289\approx)2^{18.5}$개와 $(2116\cdot\frac{7.5}{26}\cdot2\approx)2^{115.21}$의 암호화 과정으로 복구할 수 있다. 이 때는 처음에 추측한 $K[0]$ 32-bit와 $K[2], K[3]$ 각각의 32-bit 그리고 $K[1]$의 20-bit를 복구하게 된다. 비슷한 방법으로 27 라운드부터 52 라운드까지의 26라운드 XTEA에 대한 공격 또한 가능하다.

III. 결론

이상에서 블록암호 XTEA에 대해, 부정차분공격을 개선한 연관키를 이용한 차분공격에 대하여 설명하였다. 그리고 이 공격에서 필요한 선택평문과 암호화 과정은 각각 218.5과 2115.21이었다. 즉, 26라운드로 줄인 XTEA에서는 전수조사보다 효과적인 공격이 가능하다. 앞으로 블록암호분석에 있어서 연관키를 이용한 공격방법이 많이 사용될 것으로 예상된다.

다음의 표 3은 이 논문에서 언급한 다양한 형태의 XTEA에 관한 연관키 공격을 요약한 것이다.

표 3. XTEA의 다양한 라운드에 대한 공격

Rounds	Key Bits
25:1R~25R	K[0],K[2],K[3]:32bits, K[1]:15bits
26:9R~34R	K[0],K[2],K[3]:32bits, K[1]:20bits
26:27R~52R	K[0],K[1],K[3]:32bits, K[2]:15bits

참고문헌

[1] J. Kelsey, B. Schneier, and D. Wagner, "Key schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES" Advances in Cryptology-CRYPTO'96,Springer-Verlag, 1996, pp.237-251.

[2] S.Hong, D.Hong, Y.Ko, D.Jang, W.Lee, and S.Lee, "Differential Cryptanalysis of TEA and XTEA" ICISC'03, To appear.

[3] J. Kelsey, B. Schneier, and D. Wagner, "Related Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", ICICS'97, LNCS1334, 1997, pp. 203-207.

[4] D. Moon, K. Hwang, W. Lee, S. Lee, and J. Lim, ''Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA", FSE 2002, LNCS 2365, Springer-Verlag, 2002, pp.

49-60.
[5] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys.", Advances in Cryptology-EUROCRYPT'93, Springer-Verlag, 1994, pp. 398-409.
[6] D. J. Wheeler and R. M. Needham, ''TEA, a Tiny Encryption Algorithm", FSE'94, LNCS 1008, Springer-Verlag, 1994, pp. 97-110.
[7] R.M.Needham and D. J. Wheeler, ''eXtended Tiny EncryptionAlgorithm", October, 1997.
[8] A.Biryukov, D.Wagner, "Slide Attack" FSE'99, LNCS 1636, Springer-Verlag, 1999, pp. 245-259.
[9] G.Jakimoski and Y.Desmedt "Related Differential Cryptanalysis of 192-bits Key AES Variants", SAC'03, To appear.