부정차분을 이용한 전력분석공격 향상

Performance Improvement of Power attack with Truncated Differential Cryptanalysis

강 태 선, 김 희 석, 김 태 현, 김 종 성, 홍 석 희*
(Tae-Sun Kang, Hee-Seok Kim, Tae-Hyun Kim, Jong-Sung Kim and Seok-Hie Hong)

Abstract : In 1989, Kocher et al. introduced Differential Power Attack on block ciphers. This attack allows to extract secret key used in cryptographic computations even if these are executed inside tamper-resistant devices such as smart card. Since 1989, many papers were published to improve resistance of DPA. At FSE 2003 and 2004, Akkar and Goubin presented several masking methods to protect iterated block ciphers such as DES against Differential Power Attack. The idea is to randomize the first few and last few rounds(3 ~ 4 round) of the cipher with independent random masks at each round and thereby disabling power attacks on subsequent inner rounds. This paper show how to combine truncated differential cryptanalysis applied to the first few rounds of the cipher with power attacks to extract the secret key from intermediate unmasked values.

Keywords: truncated differential cryptanalysis, power analysis, Hamming Weights, blind cryptanalysis

I. 서론

1998년 Kocher 등이 발표한 블록암호에 대한 전력분석 공격을 통해 암호설계자가 예측하지 못한 부가적인 정보들을 이용해 암호분석이 가능하다는 것이 알려졌고 이후 많은 논문에서 알고리즘이 수행되면서 소비되는 전력 또는 방출되는 전자기파 등을 분석하여 비밀키를 복구하는 공격기법이 알려졌다[6]. 이에 대한 대응방안으로 알고리즘 수행순서를 랜덤하게 하는 방법과 알고리즘 수행 도중에 난수로 중간값을 마스킹하는 방법들이 발표되었다. FSE 2003과 2004에서 Akkar 와 Goubin 등이 제안한 Unique Masking Method는 알고리즘이 수행되는 라운드의 전• 후반 일부 라운드에 마스킹을 적용하여 전력분석 공격(Differential Power Analysis, DPA)에 대응하는 방안을 발표하였다[2]. 이에 대해서 SAC 2006에서 Handschuh와 Preneel는 마스킹이 적용되지 않는 내부 라운드에 차분분석(Differential Cryptanalysis, DC)을 적용하여 Unique Masking Method로 마스킹된 DES 알고리즘의 라운드 키를 찾는 공격기법을 발표하였다[5]. 본 논문에서는 부정차분(Truncated Differential Cryptanalysis, TDC)을 적용하여 Handschuh와 Preneel이 제안한 방법 보다 적은 평문쌍으로 DES 알고리즘 라운드 키를 찾을 수 있는 방안을 제시하였다.

II. DES 에 적용한 Unique Masking Method

Akkar 와 Goubin 등이 제안한 Unique Masking Method 는 DES와 같은 Feistel 구조의 암호알고리즘과 AES와 같은 Substitution Permutation Network 구조를 가진 암호알고리즘의 전• 후반부 일부 라운드의 마스킹에 적용될 수 있다. Feistel 구조의 DES에 적용하기 위해서 F 함수내의 Sbox에 대해 다음 식과 같은 두 가지의 새로운 Sbox 함수를 도입시키면 4라운드까지 중간 값들을 안전하게 마스킹 할 수 있다. α값은 32 bit의 input과 output의 난수값이며 암호화 알고리즘 실행시마다 달라진다.

$$\forall x \in \{0,1\}^{48}, S_1(x) = S(x) \oplus P^{-1}(\alpha)$$
$$\forall x \in \{0,1\}^{48}, S_2(x \oplus E(\alpha)) = S(x) \oplus P^{-1}(\alpha) \quad (1)$$

그림 1은 DES 알고리즘의 전반부 4 라운드에 Unique Masking Method가 적용된 그림이며 후반부 4 라운드도 동일한 방법으로 마스킹이 된다. 이 방식이 적용되면 F 함수 연산도중 나타날 수 있는 모든 중간값은 항상 안전하게 난수값으로 마스킹이 되기 때문에 전력분석을 통해서 중간값들을 알아낸다고 해도 실제값과 연관성이 없기 때문에 안전하다고 할 수 있다.

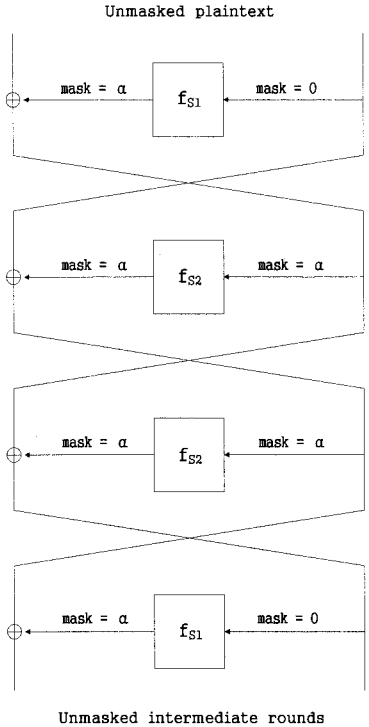


그림 1. DES 알고리즘 전반부 4 라운드에 적용된 UMM
Fig. 1. DES algorithm first 4 rounds applied with UMM.

* 책임저자(Corresponding Author)
논문접수 : 2008. 8. 12., 채택확정 :
강태선, 김희석, 김태현, 김종성, 홍석희 : 고려대학교 정보보호대학원
(boj12@naver.com, heeseokkim, thkim, joshep, hsh@cist.korea.ac.kr)
※ "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

III. 차분분석을 적용한 전력분석 공격

Biham과 Shamir가 제안한 차분분석은 DES 알고리즘의 Sbox의 입력 출력쌍이 어떤 확률을 가지고 정해진 차분을 따라서 발생하는 취약점을 이용한 분석방법이다. Handschuh와 Preneel이 제안했던 차분특성을 이용한 전력분석 공격방법은 앞 뒤의 일부 라운드에 Unique Masking Method가 적용된 DES 알고리즘에서 마스킹이 적용되지 않은 라운드에서의 차분특성과 그 차분특성을 만족시키는 평문의 Hamming weight 값을 이용한다. 차분특성에 부합하는 올바른 평문(right pair)을 Hamming weight 값으로 선별하고 그 평문들의 Hamming weight 정보를 이용해서 해당 라운드 키를 추출하는 공격방법이다. 우선, 마스킹되어 있지 않는 라운드를 선택한다. 만약 첫 번째 라운드부터 네 번째 라운드까지 마스킹이 되어 있다고 했을 때 네 번째 라운드의 F 함수 결과 값은 세 번째 라운드의 입력 값과 xor 해서 마스킹이 없어지게 된다(그림 1 참조). 결과적으로 네 번째 라운드 결과 값은 고유한 차분특성을 가지게 되고 이 특성과 전력분석에서 얻을 수 있는 정보를 통해 해당 라운드 키를 추출할 수 있다.

4라운드 차분특성을 만족하는 다수의 평문쌍에 대해서 4라운드 입력값의 hamming weight 값으로 선별한다. 4라운드의 차분특성을 P' = 405C0000 04000000 , C' = 04000000 00540000라 할 때 차분확률은 3.8×10^{-8} 이 되고 4라운드 함수의 S3 box와 S4 box의 차분특성은 0xA → 0x1와 0x28 → 0x0가 된다. 나머지 S box의 차분특성은 0x0 → 0x0이다. 우선 4 라운드 S3 box input 차분이 0xA이기 때문에 이를 Hamming weight 관점에서 보면 다음과 같은 관계식이 성립한다.

$$\mathbf{hwt}(\delta)=2 : \mathbf{hwt}(x_i)=\mathbf{hwt}(x_i') \pm 2 \text{ 또는 } \mathbf{hwt}(x_i)=\mathbf{hwt}(x_i') \quad (2)$$

이 식에서 δ 는 입력차분값으로 001010값이며 x_i 와 x_i' 은 S box 입력 평문쌍이다. 위 식을 만족시키는 평문쌍을 공격에 사용될 옳은 평문쌍으로 선별한다. S4 box의 경우에도 입력차분이 28_x이므로 위 식과 유사한 관계식이 성립하고 그 식을 이용해서 옳은 평문쌍을 선별한다. 입력차분이 δ = 101000 일 때 hwt(δ) = 2 가 되기 때문에 (2)와 같은 식이 성립한다.

S box의 입력 차분의 Hamming height 값이 2 일 때 (2)의 식이 성립하고 이 식을 만족시키는 평문쌍의 Hamming weight 종류는 17 가지가 된다. S3 box의 경우 차분특성의 확률이 10/64이므로 이 차분특성을 만족시키는 입력쌍(x_i, x_i')은 10개가 존재하고 이 입력쌍의 Hamming weight 분포는 각 S box의 라운드 키 값에 대해서 일정한 분포를 갖게 된다. 즉, 라운드 키값 각각에 대해서 독특한 분포를 갖게 되고 이 독특한 분포를 이용해서 라운드 키를 복구할 수 있다. S4 box의 차분특성 확률은 16/64이고 이 차분특성을 만족시키는 입력쌍(x_i, x_i')은 16개가 존재한다. S3 box의 Hamming weight 분포와 S4 box의 Hamming weight 분포가 서로 다르기 때문에 분포의 차이로 인해 서로 다른 키 값을 검출해 낼 수 있다. 옳은 평문쌍 선별시 hamming weight 값만을 이용하기 때문에 틀린 평문쌍이 옳은 평문쌍으로 잘못 선별될 수도 있으나 25쌍 이상의 평문쌍이 수집되고 그 평문쌍의 Hamming weight 값 분포가 구해지면 이 분포와 각 각 키 값(0 ~ 63)에서의 평문쌍 분포를 서로 비교해서 최대한 유사한 분포를 보이는 키를 옳은 키 값으로 본다. 다른 차분특성을 이용하여 S3 box와 S4 box외의 다른 S box에 대해 동일한 공격방법을 반복하여 전체 라운드 키를 복구할 수 있다.

IV. 부정차분분석을 적용한 전력분석 공격

차분특성과 전력분석을 결합한 공격기법은 제한된 라운드에 적용된 어떠한 마스킹 기법에도 적용이 가능하기 때문에 상당히 유효한 공격 기법이기는 하나 옳은 키 값을 추출하기 위해서는 2^{16}개의 평문쌍이 필요하게 되고 이 평문쌍에 대한 정확한 Hamming weight 측정을 통해 옳은 평문쌍을 선별해야한다. 이를 실제 실험과 결부시켜 생각해 보면 2^{16} 쌍의 평문에 대해 Hamming weight 오류없이 정확히 측정한다는 것이 쉽지 않은 일임을 알 수 있다. 따라서 필요한 평문쌍의 개수를 최소화할 필요가 있으며 부정차분특성을 이용하면 필요한 평문쌍 개수를 최소화할 수 있다. 부정차분 공격은 1994 년 Lars R. Knudsen 에 의해 제시된 공격 방법으로 출력값 모두를 예측하지 않고 공격에 필요한 비트 정보들만을 예측하여 공격하는 개념이 부정 차분 공격이다[1]. 이렇게 필요한 특정 비트의 정보만을 예측하기 때문에 필요한 비트 외의 정보는 랜덤한 값을 가지는 차분 특성 모두가 이 공격에 사용 가능하고 이런 관점에서 부정 차분 특성은 차분 특성 중 필요한 비트들의 값이 같은 여러 차분 특성들을 합쳐 놓은 것으로 볼 수 있다. 따라서 차분 공격에 사용되는 차분 특성보다 훨씬 높은 확률의 특성을 찾을 수 있다. 결국 확률이 높아짐에 따라 공격에 요구되는 평문쌍 개수의 수가 현저히 줄어드는 장점이 있다.

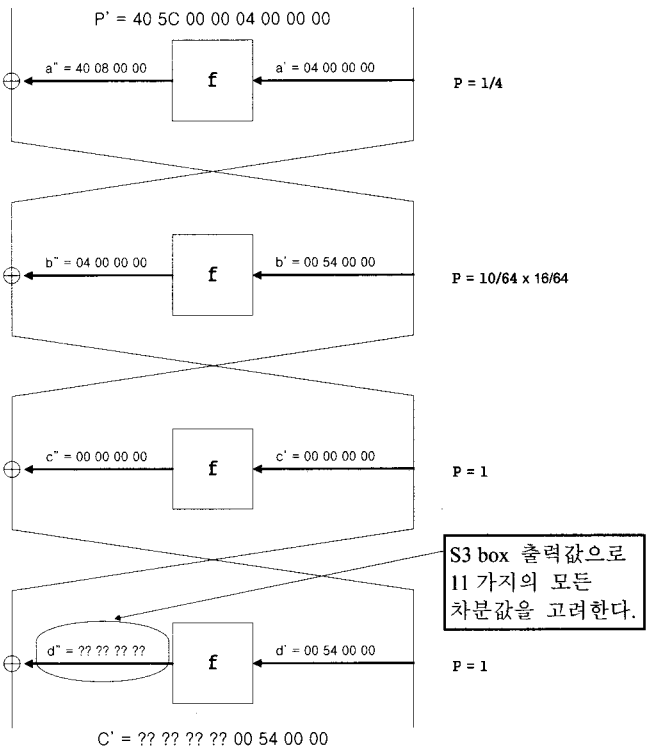


그림 2. 4 라운드 F 함수 S3 box에 부정차분 적용

Fig. 2. 4th round S3 box applied with truncated differential attack.

V. 시뮬레이션

제안한 공격기법의 효용성을 비교하고 위해 PC와 matlab를 사용하여 소프트웨어로 시뮬레이션을 수행하였다. 공격하는 S box의 Hamming weight 값은 정확히 측정할 수 있다고 가정한다. 이 가정은 실제 실험을 고려할 때도 반복 실험을 통해 충분히 정확히 측정할 수 있다고 볼 수 있다.

DES 알고리즘의 4라운드 F 함수 출력값으로 11가지가 올 수 있기 때문에 11가지의 모든 출력값이 다음 5라운드 입력에 영향을 미치게 되는데(그림 2 참조) 5 라운드 F 함수에 입력되는 전체 값을 보면 S3 box에만 차분이 모두 '0'이고 다른 S box에는 경우에 따라 '0' 또는 '1'의 차분 값을 갖는다. 이를 정리하면 표 1과 같다.

표 1. 4라운드 S 3box 출력 차분에 따른 5 라운드 S box별 입력 차분값

Table 1. 5^{th} round S boxes input characteristic corresponding to 4^{th} round S3 box output characteristic.

	S1	S2	S3	S4	S5	S6	S7	S8
1x	0	1	0	0	0	0	0	0
2x	1	0	0	0	0	0	0	1
4x	0	0	0	1	1	0	0	0
5x	0	1	0	1	1	0	0	0
6x	0	0	0	1	0	0	0	1
8x	0	0	0	0	0	1	1	0
9x	0	1	0	0	0	0	1	0
Ax	0	0	0	0		1	1	1
Cx	0	0	0	1	1	1	1	0
Cx	0	0	0	1	1	1	1	1
Fx	0	1	0	1	0	1	1	1

표 1 결과값에 따라 공격에 사용할 평문쌍을 선별한다. 선별된 평문쌍의 4 라운드 입력 Hamming weight 값을 가지고 III장에서 언급한 공격 방법으로 S3 box를 공격하여 라운드 키를 추출한다. 기존의 차분특성을 적용한 공격이 S3 box 라운드 키 하나를 알아내는데 2^{16} 개의 평문쌍이 필요했으나 부정차분특성을 적용하면 2^{8} 개의 평문쌍만이 필요하게 된다.

VI. 결론

차분특성을 이용하면 Unique Masking Method가 적용된 DES 알고리즘의 라운드키를 복구할 수 있는데 이 때 차분특성에 따라 많은 평문쌍이 필요하게 된다. Hamming weight 의 정확한 측정이 어려움점을 감안했을 때 실제 실험에서 이러한 공격은 평문쌍이 더 필요할 것으로 예상된다. 본 논문에서는 평문쌍을 줄이기 위해 부정차분 특성을 적용하였다. 부정차분을 적용하였으며 실제 시뮬레이션을 통해 공격에 필요한 평문쌍을 2^{16} 개에서 2^{8} 개로 줄일 수 있음을 확인하였다. 향후에는 좀더 효율적인 부정차분을 구한다면 공격에 필요한 평문쌍을 대폭 줄일 수 있을 것으로 판단된다.

참고문헌

[1] L. R. Knudsen, "Truncated and Higher Order Differential", *fast Software Encryption Workshop 94*, LNCS 1008, Springer-Verlag, pp. 229-236, 1995.

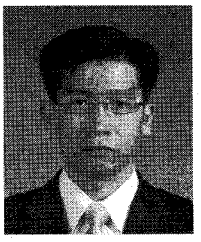
[2] M.. L. Akkar, R. Bevan and L. Goubin, "Two Power Analysis Attacks against One-Mask Methods." In: Roy, B.K., Meier, W. (eds.) *FSE 2004*. LNCS, vol. 3017, pp.332 - .347. Springer, Heidelberg (2004)

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *J. Cryptology* 4(1), 3- .72 (1991)

[4] National Institute of Standards and Technology (NIST) FIPS Publication 46-3:Data Encryption Standard (1999)

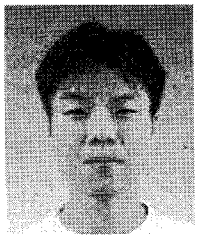
[5] H. Handschuh and B. Preneel, "Blind Dfferential Cryptanlysis for Enhanced Power Attacks," *SAC 2006*, LNCS 4356, pp. 163-173, (2007)

[6] P. Korcher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," *Technical Report, Cryptography Research Inc.*, 1998, Available from http://www.cryptography.com/dpa/technical/index/html



강 태 선

1996년 한국항공대학교 항공기계공학과 (공학사) 졸업. 20070년~현재 고려대학교 정보보호대학원 석사과정 재학 중. <관심분야> 부채널 공격,



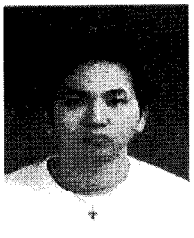
김 종 성

2000년 고려대학교 수학과 학사.
2002년 고려대학교 수학과 석사
2006년 K.U.Leuven, ESAT/SCD-COSIC 박사. 2007년 2월 : 고려대학교 정보보호대학원 박사. 2007년 3월 ~ 2008년 3월 : 고려대학교 정보보호연구원 박사후연구원. 2008년 4월 ~ 현재 고려대학교 정보보호연구원 연구교수. <관심분야> 암호 알고리즘 설계 및 분석

홍 석 희

1995년 고려대학교 수학과 학사. 1997년 고려대학교 수학과 석사. 2001년 고려대학교 수학과 박사. 1999년~2004년 (주)시큐리티 테크놀로지스 선임연구원. 2003년~2004년 고려대학교 시간강사. 2004년~2005년 K.U. Leuven 박사후연구원. 2005년~현재 고려대학교 정보경영전문대학원 조교수. <관심분야> 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식등

.



김 희 석

2006년 연세대학교 수학과 졸업(이학사). 2008년 고려대학교 정보경영공학전문대학원 졸업(공학석사). 2008년 ~ 현재: 고려대학교 정보경영공학전문대학원 박사과정 재학 중.
<관심분야> 부채널 공격, 공개키 암호시스템 안전성 분석 및 고속구현, 타원곡선 알고리즘

김 태 현

2002년 서울 시립대학교 수학과 졸업 (이학사). 2004년 8월: 고려대학교 정보보호 대학원 졸업(공학석사). 2005년 ~현재 고려대학교 정보경영공학전문대학원 박사과정 재학 중. <관심분야> 부채널 공격, 공개키 암호 알고리즘, 암호칩 설계 기술

.