차분 전력 분석에서 분류함수의 위치가 성공확률에 미치는 영향*

김 성 경[1], 김 희 석[1], 김 태 현[1], 한 동 국[2], 류 정 춘[1], 임 종 인[1]
[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원
likesk@cist.korea.ac.kr

The effect which the location of Partitioning Function causes in successful probability in Differential Power Analysis

Sung-Kyoung Kim[1], HeeSeok Kim[1], Tae Hyun Kim[1], Dong-Guk Han[2],
Jeong Choon Ryoo[1], Jongin Lim[1]
[1]Graduate School of Information Management and Security, Korea University,
[2]Electronics and Telecommunications Research Institute

요약

최근 부채널 공격으로 스마트 카드 같은 장치의 비밀키를 알아낼 수 있음이 알려지면서 많은 알고리즘에 대한 부채널 공격과 대응 방안이 연구되고 있다. 차분전력분석은 부채널 공격의 일종으로 암호화 연산 중 발생하는 전력 소모 곡선을 통계적으로 분석하여 키를 알아내는 공격이다. 본 논문에서는 Kocher 형태의 IC칩 차분전력분석공격에 대한 실험 분석 모델을 설정한 후 이를 검증하고자 축소형 모델로 실험한다. 실험 분석을 위하여 선정된 장치에 DES 암호 알고리즘을 어셈블리로 구현한 후 8비트 마이크로프로세서 형 칩에 탑재하여 암호 알고리즘 실행 시에 발생되는 차분 전력 신호를 분석한다. 그리고 차분전력분석 공격에서 중요한 기술인 분류함수 설정에 따른 분석 성공 여부에 따른 비교를 한다.

1. 서론

현재 인터넷과 전자상거래의 급속한 성장으로 인터넷 뱅킹, 전자화폐, 의료카드, 교통카드 및 전자주민통합카드 등 전자상거래 개인 인증 솔루션으로 적합하다는 평가를 받고 있는 스마트 카드[1,3,8,9]는 안전한 개인정보의 저장, 개인키의 저장, 그리고 개인 인증서 저장 등의 수단으로 많이 활용될 수 있다. 특히 기존의 자기 카드와 달리 마이크로프로세서와 메모리 기능을 내장한 스마트 카드는 물리적인 보안성이 뛰어나고 안전한 개인 정보를 저장하는 수단으로 적합할 뿐 아니라 저장성, 연산 기능, 보안기능을 포괄한 다기능 카드로 활용이 높다.

한편, 암호 알고리즘의 설계 시 고려하지 못한 부채널 정보가 존재하는 것으로 알려지고 있다[7,8]. 이러한 부채널 정보로는 마이크로프로세서의 작동 시 키 값이 "0"/"1"에 의한 시간 작동 차이를 나타내는 시차정보, 전력선으로부터 누출되는 신호정보, 결함 주입으로 발생되는 오작동 정보, 전자기 누출에 의한 정보 등으로 분류될 수 있다. 부채널(side-channel)[10,11]에 의한 스마트 카드 공격 기술을 일반적으로 부채널 공격(side-channel attack)이라고 부른다. 이 중에서 전력분석공격[4,5,6,9,10]은 단순 전력 분석(simple power analysis), 차분 전력 분석(differential power analysis)으로 대별된다. 전력 분석 공격은 카드 내부에 내장된 암호 알고리즘과 암호용 비밀키가 작동되는 순간에 IC 칩의 순간적인 전압 (전력)변화를 관측하여 각종 정보의 이진 코드를 읽어낸 후 통계적인 방법으로 중요 정보 분석은 물론 위·변조까지 가능한 암호해독 기술이다. 차분전력분석 기술은 전압변화를 관측할 수 있는 몇 가지 장치만 구비하면 비밀키의 추정이 가능하기 때문에 전용의 해독기계 또는 슈퍼컴퓨터를 동원한 전수공격(brute-force attack) 보다 훨씬 효과적인 것으로 분석되고 있다. 이러한 차분전력분석 기술이 개발되면서 전자상거래(EC) 분야의 지불수단 안전성 문제와 함께 국내외 스마트 카드 제조사와 IC 칩 기반 카드업계의 제품생산 계획 자체도 위협 받고 있는 실정이다.

본 논문에서는 Kocher 형태의 IC칩 차분전력분석 공격에 대한 실험 분석 모델을 설정한 후 이를 검증하고자 축소형 모델로 실험한다. 실험 분석을 위하여 선정된 장치에 DES 암호 알고리즘[2]을 어셈블리로 구현한 후 8비트 마이크로프로세서 형 칩에 탑재하여 암호 알고리즘 실행 시에 발생되는 차분 전력 신호를 분석한다. 그리고 차분전력분석 공격에서 중요한 기술은 분류함수를 어떻게 설정하는가 하는 점이며, 이러한 여러 가지 분류함수에 대한 분석 성공 여부를 비교한다.

2. 부채널 공격

부채널 공격[7,8]이란 암호 시스템이 내장된 장치에서 암호 알고리즘이 실행될 때 발생하는 부가 정보를 이용하여 장치 내에 내장된 비밀정보를 알아냄으로써 암호시스템을 공격하는 방법이다. 이 중에서 전력 분석 공격[4,5,6,9,10]은 암호 장치가 연산을 수행하는 동안 소모하는 전력의 추이를 관찰함으로써 비밀키를 찾아낸다. 전력 분석 공격은 단순전력분석 (simple power analysis, SPA) 공격과 차분전력분석 (differential power analysis, DPA) 공격, 크게 두 가지로 나뉠 수 있다.

* "본 연구의 일부는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2006-(C1090-0603-0025))

가. 단순 전력 분석 공격

단순 전력 분석 공격 (SPA)은 암호 시스템에서 연산되는 암호 프로세서의 전력소비를 관찰하여 내부에 저장되어 있는 비밀키를 직접 공격하는 방법이다. 프로세서의 명령에 따라 각기 다른 전력을 갖는 다는 사실을 암호 시스템 외부에서 관찰할 수 있으며 이로부터 키 또는 순간 작동 중인 명령에 대한 정보를 추론하는 공격 방법이다.

나. 차분 전력 분석 공격

차분 전력 분석 공격 (DPA)은 SPA보다 방어하기 어려운 공격 방법이며, SPA가 소비 전력을 관찰하는 것에 반하여 DPA는 비밀키와 정확히 상관관계를 가지는 정보를 추출하기 위해 통계적인 분석과 에러정정 기술을 사용한다. 즉, 암호 시스템에서 암호 연산 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음 표본화된 데이터로부터 잡음신호를 감소시키고 차분 신호의 명확성을 높이기 위해서 디지털 신호 해석 및 통계기법을 적용하여 분석하는 공격이다. DPA 공격방법은 전력소비 데이터를 수집한 후 이를 분석하기 위하여 통계적인 분석방법을 사용하여야 한다. 먼저 정확한 비밀키가 들어갔을 때 그 비밀키와 반응을 알 수 있는 분류함수 또는 선택함수를 정해야 하는데 이 함수는 특정비트나 바이트의 해밍웨이트를 조사하여 데이터 수집단계에서 수집한 데이터를 분류하는 함수이다. 이러한 분류함수로 데이터를 적절히 분류한 후 가능한 비밀키의 집합에서 키를 추측하여 통계적인 방법으로 비밀키를 찾아 낼 수 있으며, 다음은 Kocher 형태의 DPA 공격 단계를 나타내었다.

① 전체 구하려는 스마트 카드의 n 비트 비밀키 K를 $(k_n,\cdots,k_1,k_0)$라 정의하고, 최상위 혹은 최하위 비트의 순서로 순차적으로 키의 일부가 입력되어 연산된다고 가정한다.

② 먼저 키의 일부인 k_i를 미리 가능한 키 영역에서 추측한다.

③ 추측한 키와 전력신호 데이터를 구할 때 쓴 평문을 입력으로 연산을 수행한 후 분류함수를 이용하여 전력신호 데이터를 분류한다.

S_0={Ci[j] | D(key, data)=0 or low hamming weight}

S_1={Ci[j] | D(key, data)=1 or high hamming weight}

④ 양분한 데이터를 각각 평균하여 차분신호를 구한다.

$$\Delta_D[j]=\frac{1}{|S_0|}\sum_{S_i[j]\in S_0}S_i[j]-\frac{1}{|S_1|}\sum_{S_i[j]\in S_1}S_i[j]$$

⑤ 평문과 전력소비신호의 수가 많을 시 추측한 키가 옳다면 $\Delta_D[j]$ 신호가 거의 0에 수렴한다. 키가 반응하는 지점에서 non-zero 이고 추측한 키가 맞지 않는다면

$$\lim_{t\to\infty}\Delta_D[j]\approx \text{non-zero} \quad \text{if guess is correct}$$

$$\lim_{t\to\infty}\Delta_D[j]\approx 0 \quad \text{if guess is incorrect}$$

⑥ 추측이 옳지 않다면 다시 ②로 돌아간다.

⑦ 추측이 옳다면 그 키가 실제 내부 키 일부가 된다.

⑧ 나머지 키에 대하여 ②~⑦과정을 계속 반복하여 전체 키를 찾는다.

상기 과정을 계속 반복하여 내부에 내장된 전체 키 값을 찾을 수 있다. 각각 하나의 Δ_D에 대하여 가능한 키를 모두 입력한 다음 그 중에 하나인 실제 키를 찾는 방법이다. DPA 공격에서 중요한 기술은 분류함수인 D(key, data)를 어떻게 설정하는가 하는 점이며, 구현된 암호 알고리즘에 따라 설정 방법이 큰 차이가 있을 수 있다.

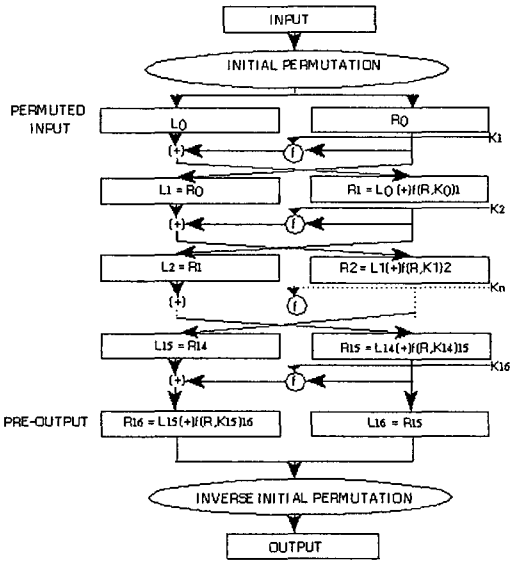
3. DES에 대한 차분 분석 공격

본 장에서는 부채널 공격 실험에 사용 된 DES에 대한 차분 분석 공격을 설명한다.

가. DES의 구조

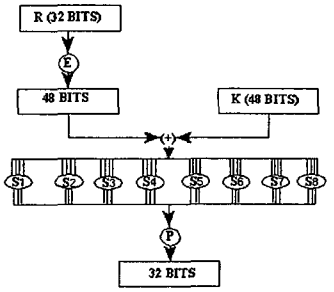
DES(Data Encryption Standard)[2]암호는 암호키와 복호키가 같은 대칭키 암호로 1960년대 말에 IBM에서 개발하여 1977년 미국 표준 암호 알고리즘으로 채택되어 속도가 빠르기 때문에 금융기관 등 여러 분야에서 세계적으로 사용되고 있는 암호이다. DES암호는 대칭 블록 암호로서 평문의 각 블록의 길이가 64비트이고 키가 64비트(실제로는 56비트가 키이고 8비트는 검사용)이며 암호문이 64비트인 암호이다.

DES 알고리즘은 64비트의 평문이 16라운드의 Feistel 연산을 거쳐 64비트의 암호문이 나오게 하는 것이다. 전체적인 구성은 아래 [그림 1]과 같다. Li, Ri는 각각 32비트이고, L_0, R_0는 평문의 Initial Permutation 결과를 32비트씩 나누어 상위비트를 L_0, 하위비트를 R_0라고 한다.



[그림 1] DES의 전체적인 구도

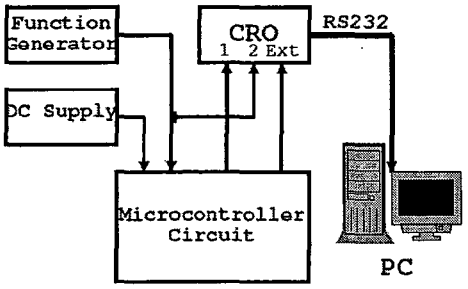
이 때 각 라운드마다 수행하는 F함수는 [그림 2]와 같다. E는 Expansion Permutation으로 32비트를 48비트로 확장하고, Si들은 S-box Substitution으로 확장된 48비트를 8 토막으로 나누어 다시 32비트로 바꾸게 된다. 마지막 P는 P-box Permutation으로 32비트를 자리만 바꾼다.



[그림 2] DES의 F함수

나. 실험 환경

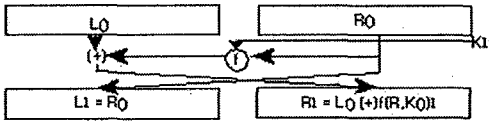
실험 대상이 되는 암호 시스템은 PIC micro-controller을 사용한다. 실험에 사용한 칩은 기본적으로 8비트 연산을 수행하며, DES는 어셈블리 언어로 구현되어 있다. 이 때, DES의 키는 PIC칩에 저장되어 있고 암호문의 값이 다음 평문의 입력값으로 사용된다. PIC칩의 동작을 위해서는 전력과 클럭이 사용되어야 한다. 본 실험에서는 DC Power Supply를 이용하여 +5V의 전력을 외부에서 공급하고, Function generator를 이용하여 1MHz의 sine wave를 공급하게 된다. 그리고 소비전력파형을 측정하기 위하여 Tektronix사의 TDS3032B의 오실로스코프(CRO)를 사용한다. 측정한 파형 분석은 Visual C++을 이용한다. [그림 3]은 전체 실험 환경에 대한 도식화이다.



[그림 3] 차분 전력 분석 공격 실험 환경

다. 실험 과정과 실험 결과

DES에 대한 차분 전력 분석 공격은 헤밍웨이트 모델을 기본 가정으로 하고 있으며, 각 라운드의 결과 값이 저장되는 시점을 알고 있다고 가정한다. DES는 [그림 4]의 R1 계산 과정에서 공격자가 F함수의 입력과 출력을 알고 있으면 라운드 키를 구할 수 있으므로 차분 전력 분석 공격에 취약하다.



[그림 4] 1 라운드 DES에 대한 차분전력분석 공격

먼저 공격자는 분류함수 $D(L_0, R_0, K_1)=L_0 \; XOR \; S1(R_0 \; XOR \; K_1)$를 정의한다. 이 때, L_0는 평문의 상위 32비트 중에서 F함수의 결과 값 중 1비트와 XOR되는 1비트를 나타내고, R_0는 평문 하위 32비트 중에서 첫 번째 S-box의 입력 값 6비트를 의미하고 K_1은 1 라운드 키 중에서 첫 번째 S-box의 입력 값 6비트를 의미한다. 공격 수행 방법은 2.나.에서 살펴본 것과 동일하다.

① 위에서 정의한 분류함수를 이용하여 전력신호 데이터를 분류한다.

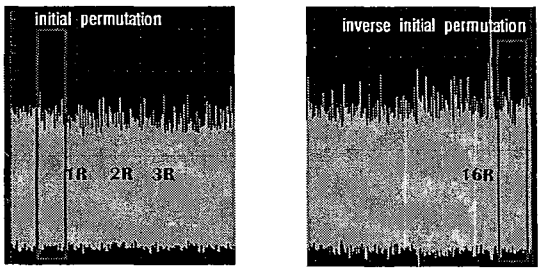
$S_0=\{Ci[j] \mid D(L_0, R_0, K_1)= 0\}$

$S_1=\{Ci[j] \mid D(L_0, R_0, K_1)= 1\}$

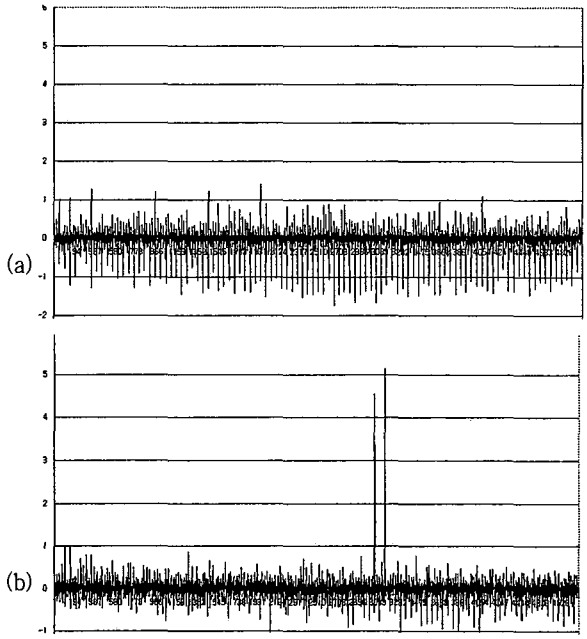
② 양분한 데이터를 각각 평균하여 차분신호를 구한다.

$$\Delta_D[j]=\frac{1}{|S_0|}\sum_{S_i[j]\in S_0} S_i[j]-\frac{1}{|S_1|}\sum_{S_i[j]\in S_1} S_i[j]$$

만약 K_1이 잘못된 키이면 분류함수의 값이 난수발생기와 같은 동작을 하게 된다. 이는 실제 비밀키가 어떤 상관관계도 갖고 있지 않기 때문이다. 반면에 올바른 키를 추측하였다면 분류함수를 통해서 계산된 값이 일치하기 때문에 분류함수는 상관관계를 가지게 되므로 그 결과 power trace의 차분은 non-zero의 값을 가지게 된다. [그림 5]는 DES 알고리즘을 PIC에 탑재한 후 1000번씩 수행하여 측정한 평균 소비 전력 파형이고, [그림 6]은 DES의 전력분석 공격을 적용하였을 경우 결과이다. (a)는 잘못된 키를 추측하였을 경우이고, (b)는 올바른 키를 추측하였을 경우이다.



[그림 5] DES의 평균 파형



[그림 6] DES의 차분전력분석 결과

4. 분류 함수와 분석 성공률과의 관계

3장에서 살펴본 것과 같이 차분전력분석 공격을 하기 위해서는 먼저 공격자가 알고리즘에 맞는 분류함수를 정의해야 한다. DES의 경우 대표적인 분류함수는 3.다에서 정의 한 것과 같이 S-box의 출력 값과 평문 상위 48비트와의 XOR의 결과 값을 이용하여 전력신호 데이터를 분류하게 된다. 본 장에서는 이러한 분류 함수의 위치를 바꾸었을 경우 키를 찾을 수 있는 확률, 즉 분석 성공률의 관계를 알아보려고 한다. 먼저 DES에서 가능한 분류함수 3가지를 생각해 본다.

① $D1(L_0, R_0, K_1)=L_0 \; XOR \; S1(R_0 \; XOR \; K_1)$

D1은 3장에서 소개한 분류함수이다. 다시 말해서 S-box의 출력 값과 평문의 XOR의 결과 값을 이용하여 분류한다. 즉, L_0, R_0, 2개의 평문을 이용하게 된다.

② $D2(R_0, K_1)=S1(R_0 \; XOR \; K_1)$

D2는 D1의 분류함수에서 S-box의 결과 값만을 이용하는 것이다. 즉, D1과는 달리 한 개의 평문을 이용하게 된다.

③ $D3(R_0, K_1)=R_0 \; XOR \; K_1$

D3은 S-box의 결과 값을 사용하지 않는 경우이다. D1과 D2와는 달리 이 경우의 공격방법은 K1을 0이라고 가정한 다음 D3(R0, K1)의

값이 0과 1인 경우로 분류한다. 양분한 데이터의 평균하여 차분신호를 구한 후 차분 신호 값이 음수이면 키의 값은 0이고, 양수의 경우는 키 값이 1이 된다.

아래 [표 1]은 3가지 분류함수에 따른 공격 성공 확률을 나타낸 것이다. S1~S8은 8개의 S-box이고 O/X는 키 성공 여부이다. 100~1000의 수는 PIC칩에서 수행한 횟수이다.

(a)

	1000	900	800	700	600	500	400	300	200	100
S1	O	O	O	O	O	O	X	O	O	X
S2	O	O	O	O	O	O	X	X	X	X
S3	O	O	O	O	O	O	O	X	X	X
S4	O	O	O	O	O	X	X	X	X	X
S5	O	O	O	O	O	O	O	O	X	X
S6	O	O	O	O	O	X	X	X	X	X
S7	O	O	O	O	O	O	O	X	X	X
S8	O	O	O	O	O	O	O	X	X	X

(b)

	1000	900	800	700	600	500	400	300	200	100
S1	O	O	X	X	X	X	X	X	X	X
S2	O	X	X	X	X	X	X	X	X	X
S3	O	X	X	X	X	X	X	X	X	X
S4	O	O	X	X	X	X	X	X	X	X
S5	O	X	X	X	X	X	X	X	X	X
S6	O	O	X	X	X	X	X	X	X	X
S7	O	X	X	X	X	X	X	X	X	X
S8	O	X	X	X	X	X	X	X	X	X

(c)

	1000	900	800	700	600	500	400	300	200	100
S1	O	X	X	X	X	X	X	X	X	X
S2	X	X	X	X	X	X	X	X	X	X
S3	X	X	X	X	X	X	X	X	X	X
S4	X	X	X	X	X	X	X	X	X	X
S5	X	X	X	X	X	X	X	X	X	X
S6	X	X	X	X	X	X	X	X	X	X
S7	X	X	X	X	X	X	X	X	X	X
S8	X	X	X	X	X	X	X	X	X	X

[표 1] D1, D2,,D3의 분류함수를 사용하였을 경우 성공 여부

[표 1]에서 알 수 있듯이 본 실험 환경에서는 D1의 분류 함수를 이용하여 차분전력분석을 하였을 경우 600개의 power traces(즉, 수행 횟수)를 이용하여 DES의 8개 S-box의 모든 키를 알아낼 수 있고, D2의 분류함수의 경우 1000개의 traces를 이용하여 DES의 키를 알아낼 수 있다. D3의 분류함수의 경우 1000개의 traces를 이용할 경우 첫 번째 S-box의 키만을 알아 낼 수 있다.

본 실험에 따른 결과는 실험 환경과 분석 대상을 어떻게 구현하였는지에 따라 차분전력분석 공격에서 분류함수의 위치에 따른 성공 확률이 달라질 수 있다고 추측할 수 있다. 즉, PIC칩이 전력을 소모하는 CMOS의 동작 원리에 따라서 그리고 타겟 대상 알고리즘을 어셈블리 언어로 구현한 방법에 따라서 성공확률도 달라질 수 있다.

5. 결론 및 향후 연구에 대한 제안

본 논문에서는 스마트 카드 암호 해독을 위하여 Kocher 형태의 DPA 공격 실험분석 모델을 선정하여 이를 축소하여 실험을 실시하였다. 실험 분석을 위하여 선정된 장치에는 DES 암호 알고리즘을 어셈블러로 구현 한 후 8비트 마이크로프로세서 형 칩에 탑재하였고, 암호 알고리즘 실행 시에 발생되는 차분전력신호를 수집/ 분석하였다. 이를 위하여 1000개 전력 샘플 데이터를 수집하여 전력 분석 공격 실험을 실시하였고, DPA의 분석에서 중요한 과정 중 하나인 분류함수 선정에 관한 비교를 하였다. PIC칩 환경과 DES를 어떻게 구현하였는가에 따라서 달라지겠지만 본 논문에서 실시한 실험 환경에서는 2개의 평문을 사용한 분류함수에서 더 적은 샘플 데이터를 이용하여 DES의 키를 찾을 수 있다는 것을 보여주었다. 본 논문에서는 정해진 실험 환경에서의 분류함수 위치에 따른 분석 성공확률을 실험적으로 제시하였다. 앞으로 본 실험 결과에 대한 이론적인 증명과 다른 환경에서의 성공 확률에 관한 연구가 추가적으로 진행 되어야 할 것이다. 또한 D3의 분류함수에서 수행 횟수를 늘렸을 때 분석 성공 여부도 연구할만한 가치가 있다고 사료된다.

References

[1] 이만영외, "스마트 카드를 이용한 정보보호 기술에 관한 연구," 국방과학연구소 최종연구보고서, 1997.

[2] National Bureau of Standards, Data Encryption Standard, FIPS-Pub.46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[3] ISO/IEC 7816, Part 1-6, Identification Cards - Integrated Circuit(s) Card with contacts, ISO Standard.

[4] J.S. Coron, L.Goubin, "On Boolean and Arithmetic Masking against Differential Power Analysis," CHES'2000, pp.231-237, 2000.

[5] L. Goubin and J. Patarin, "DES and differential power analysis," CHES'99.

[6] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," http://cryptography.com/dpa/technical, 1998.

[7] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall, "Side Channel Cryptanalysis of Product Cipher," Proceedings of ESORICS'98, pp.97-112, Springer-Verlag, Sep. 1998.

[8] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall, "Side Channel Cryptanalysis of Product Cipher (final version)," in the site, 2000.

[9] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of Advances in Cryptology-CRYPTO'99, pp. 388-397, Springer-Verlag, 1999.

[10] Thomas S. Messerges, Ezzy A. Dabbish and Robert H Sloan, "Investigations of Power Analysis Attacks on Smartcards," Proceedings of USENIX Workshop on Smartcard Technology, pp. 151-161, May 1999.