한국산업정보학회논문지 제7권 제4호 (2002. 12)

블록 형태 암호에서의 DPA 방어기술 연구
(A Study on DPA Countermeasures of the block-type ciphers)

이 훈 재*, 최 희 봉**, 이 상 곤*
(Hoon-Jae Lee*, Hee-Bong Choi** and Sang-Gon Lee*)

요 약 본 논문에서는 스마트카드에 탑재한 암호분석기술로 평가되고 있는 부채널 공격과 가장 위협적인 전력분석공격에 대하여 살펴본 다음 DPA 분석에 대한 세부 기법을 여러 파라미터로 비교 분석하였다. 그리고 스마트카드에 DES-like 암호 알고리즘을 탑재 시에 암호해독 가능하다고 알려진 DPA 공격방법에 대응할 수 있는 소프트웨어적인 해킹방어기술을 제안하였다.

Abstract Attacks have been proposed that use side information as timing measurements, power consumption, electromagnetic emissions and faulty hardware. Elimination side-channel information or prevention it from being used to attack a secure system is an active ares of research. In this paper, differential power analysis techniques used to attack DES are compared and analyzed. Finally, we propose a software prevention idea of DPA attack for DES-like ciphers.

1. 서 론

현재 인터넷과 전자상거래의 급속한 성장으로 인터넷 뱅킹, 전자화폐, 의료카드, 교통카드 및 전자주민통합카드 등 전자상거래 개인 인증 솔루션으로 적합하다는 평가를 받고 있는 스마트카드[1-5]는 안전한 개인정보의 저장, 개인 키의 저장, 그리고 개인 인증서 저장 등의 수단으로 많이 활용될 수 있다. 특히 기존의 자기 카드와 달리 마이크로프로세서와 메모리 기능을 내장한 스마트카드는 물리적인 보안성이 뛰어나고 안전한 개인 정보를 저장하는 수단으로 적합할 뿐 아니라 저장성, 연산기능, 보안기능을 포괄한 다기능 카드로 활용이 높다.

한편, 암호 알고리즘의 설계시 고려하지 못한 부채널 정보가 존재하는 것으로 여러 문헌자료[6-7]를 통하여 알려지고 있다. 이러한 부채널 정보로는 마이크로프로세서의 작동시 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)에 의한 스마트 카드 공격 기술을 일반적으로 부채널 공격(side-channel attack)[6-7]이라고 부르며, 시차정보에 의한 시차공격(timing attack), 결함 오작동 정보에 의한 결함 주입 공격(fault-insertion attack), 전자기 누출 정보에 의한 전자기 누출 공격(electromagnetic emition attack), 그리고 전력선 누출 정보에 의한 전력분석 공격(power analysis attack)으로 대별된다. 이 중에서 전력분석공격[8-12]은 단순 전력 분석(simple power analysis), 차분 전력 분석(differential power analysis), 추론 전력 분석[14](inferential power analysis), 그리고 고차 차분 전력 분석[15](high-order differential power analysis) 공격으로 대별된다. 전력 분석 공격은 카드 내부에 내장된 암호 알고리즘과 암호용 비밀 키가 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. DPA 기술은 전압변화를 관측할 수 있는 몇 가지 장치만 구비하면 비밀 키의 추정이 가능하기 때문에 전용의 해독기계 또는 슈퍼

* 동서대학교 인터넷공학부(hjlee@dongseo.ac.kr),
** 국가보안기술연구소(hbchoi@etri.re.kr)

컴퓨터를 동원한 전수공격(brute-force attack) 보다 훨씬 효과적인 것으로 분석되고 있다. 이러한 DPA 기술이 개발되면서 전자상거래(EC) 분야의 지불수단 안전성 문제와 함께 국내외 스마트 카드 제조사와 IC 칩 기반 카드업계의 제품생산 계획 자체도 위협 받고있는 실정이다.

본 논문에서는 스마트카드에 탑재된 암호분석기술로 평가되고 있는 부채널 공격과 가장 위협적인 전력분석공격에 대하여 살펴본 다음 DPA 분석에 대한 여러 가지 파라메터를 비교 분석한다. 그리고 스마트카드에 DES-like 암호 알고리즘을 탑재 시에 암호해독 가능하다고 알려진 DPA 공격방법에 대응할 수 있는 소프트웨어적인 해킹방어기술을 제안한다.

2. 부채널 공격 비교

부채널 공격 중에서 시차공격(timing attack, TA)[16]은 스마트카드에 내장된 비밀 키 값에 따른 마이크로 코드 상에서의 동작시간상의 차이를 비교 분석하며, 오류 주입공격(fault-insertion attack, FA)[17]은 마이크로 코드 상에서의 외형적인 값(동작시간, 전력 정보 등)과 알고 있는 비교 값과의 차이를 외부에서 오류 주입을 통하여 분석하는 공격이고, 전력분석공격(power analysis attack, PA)[8]은 마이크로 코드 상에서 평문(암호문)의 입력변화에 따른 스마트카드 전력소모의 차이를 통계적으로 분석하는 공격 기법이다. 세 가지 공격은 공격 개념, 전제 조건, 분석 파라미터 및 유사 분석 등의 측면에서 비교하여 요약하면 표 1과 같다. 이들 중에서는 일반적으로 전력 분석 공격이 가장 강력한 것으로 알려져 있으며, 스마트카드 안전성 평가항목에 포함되어야 할 것으로 판단된다.

그리고 표 2에서는 표1의 전력 분석 공격을 세분하여 분석하였다. 단순 전력 분석 공격(simple power analysis attack, SPA)[8-9]은 스마트카드에서 연산되는 암호 프로세서의 전력소비를 직접 관찰하여 카드 내부에 저장되어 있는 비밀키를 알아내는 공격 방법이고, 차분 전력 분석 공격(differential power analysis attack, DPA)[8]은 스마트 카드가 암호학적 연산을 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음, 표본화된 데이터를 잡음신호 감소와 차분 신호의 명확성을 위해 디지털 신호 해석과 통계적인 방법으로 분석하는 공격 기법이다. 추론 전력 분석 공격(inferential power analysis attack, IPA)[14]은 공격자가 필요로 하는 정도의 소비전력 신호를 가질 수 없고 평문과 암호문의 쌍을 가질 수 없는 상황에서 암호 알고리즘 실행에 따른 키 비트들의 반응 시점을 종합적으로 확인한 후 키 정보를 추출하는 공격 기법이다. 상기 세 가지 공격 중에서는 일반적으로 DPA 공격이 가장 강력한 것으로 알려져 있어서 스마트카드 안전성 평가항목에 포함되어야 할 것으로 판단된다.

표 3에는 표 2의 DPA 공격을 공개키 암호에 적용하는 방법을 세분하여 분석하였다. RSA-like 암

표 1. 부채널 공격 방법 비교 요약

항목	Timing attack(TA)	Fault-insertion attack(FA)	Power analysis attack(PA)	비 고
공격 개념	스마트카드에 내장된 비밀키 값에 따른 마이크로코드상에서의 동작시간상의 차이를 비교 분석하는 공격 기법	스마트카드에 내장된 비밀키 값에 따른 마이크로코드상에서의 외형적인 값(동작시간, 전력 정보 등)과 비교 값과의 차이를 외부에서 오류주입을 통하여 분석하는 공격기법	스마트카드에 내장된 비밀키 값에 기반한 마이크로코드상에서의 전력 측정값이 여러 종류의 평문(암호문) 입력변화에 따른 전력소모의 차이로 나타남을 이용하는 통계적 데이터 분석 공격 기법	PA공격 방법이 가장 강력하다고 알려짐.
전제 조건	1) 암호시스템 제공 2) 마이크로코드 제공	1) 암호시스템 제공 2) 마이크로코드 제공 3) 알려진 키에 대한 기준 값(reference) 제공	1) 암호시스템 제공 2) 마이크로코드 제공 3) 상당수의 평문 4) 암호문쌍 제공	
분석 파라메터	임의의 키에 따른 명령어 수행 시간 차이	임의의 키에 따른 시간 또는 중간 데이터 값의 차이	임의의 키에 따른 통계적인 소모전력의 차이	
최초 제안	Paul Kocher (Cryptography Research Co., USA), CRYPTO'96 [16]	Biham & Sharmir, CRYPTO'97 [17]	Paul Kocher, Jaffe & Jun, CRYPTO'99 [8]	
유사 방법	TA	DFA (Differential Fault Attack)	1)SPA/DPA(HO-DPA)/IPA: DES-like 2)SEMD/MESD/ZEMD: RSA-like	

표 2.전력분석공격 방법 비교 요약

항목	SPA	DPA(HO-DPA)	IPA	비 고
공격 개념	스마트카드에서 연산되는 암호 프로세서의 전력소비를 직접 관찰하여 카드 내부에 저장되어 있는 비밀키를 직접 공격하는 방법	스마트 카드가 암호학적 연산을 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음, 표본화된 데이터를 잡음신호 감소와 차분 신호의 명확성을 위해 디지털 신호 해석과 통계적인 방법으로 분석하는 공격 기법	공격자가 필요로 하는 정도의 소비전력 신호를 가질 수 없고 평문과 암호문의 쌍을 가질 수 없다면, 암호 시스템이 암호 알고리즘을 실행할 때 몇 번째 키가 어디에서 반응하는지 그 시점을 확인한 후 키 정보를 추출하는 공격기법	DPA 공격 방법이 가장 강력하다고 알려짐.
전제 조건	1) 암호시스템 제공 2) 마이크로코드 제공	1) 암호시스템 제공 2) 마이크로코드 제공 3) 상당수의 평문-암호문쌍 제공	1) 암호시스템 제공 2) 마이크로코드 제공 3) 제한적인 평문-암호문쌍 제공	
분석 파라메터	단순한 소모전력	임의의 키에 따른 통계적인 소모전력의 차이	일부의 키에 따른 반응시점 정보	
최초 제안	Paul Kocher, Jaffe & Jun, '98 homepage [9] /CRYPTO'99 [8]	Paul Kocher, Jaffe & Jun, CRYPTO'99 [8]	P. Fahn and P. Pearson, CHES'99 [14]	
공격 대상	- DES-like	- DES/AES - RSA/D-H - ECC	- DES-like	

표 3. RSA에 대한 DPA 방법 비교 요약

항목	SEMD (Single-exponent, multiple data)	MESD (Multiple-exponent, single data)	ZEMD (Zero-exponent, multiple data)	비 고
공격 개념	이미 알고있는 키와 스마트카드를 이용하여 미지의 공격하고자 하는 스마트카드의 비밀키를 알아내려고 하는 공격방법	비밀 키를 사용하여 멱승 과정에서의 평균 소비전력을 구한 다음 이를 이용하여 각각에 대한 차분 데이터를 계산하여 더 긴 시간 동안 "0"이 나타나는 경우가 올바른 키로 추정하는 공격방법	특정 바이트의 해밍 중을 분류함수로 지정하여 전력을 두 부류로 분류한 후 DPA 공격 방법 적용	ZEMD 방법이 상반인격이세지에제적소선신를요함.
전제 조건	1) RSA를 공격하기 위해서는 많은 수의 소비전력 신호가 제공되어야 한다. (예, 16비트 키를 찾기 위하여 비트당 2000개의 전력 신호가 필요함) 2) 동일한 유형의 스마트카드 2매(비교용, 공격대상)	1) 공격자가 일정한 값을 자신이 선택한 지수를 사용하여 멱승과정을 수행할 수 있다. 2) 동일한 유형의 스마트카드 2매(비교용, 공격대상) 3) 비교용 스마트카드는 키 값이 수정 가능하여야 한다.	1) 공격자가 일정한 값을 자신이 선택한 지수를 사용하여 멱승과정을 수행할 수 있다. 2) 공격자는 어떤 멱지수에 대해 알 필요도 없는 대신에 오프라인 시뮬레이션을 이용하여 멱승과정에서의 중간값에 대한 결과를 예측할 수 있어야 한다. 3) 스마트카드 1매(공격대상)	
모델 최초 제안	T. S. Messerges, E.A. Dabbish, and R.H. Sloan CHES'99 [15]	T.S. Messerges, E.A. Dabbish, and R.H. Sloan CHES'99 [15]	T.S. Messerges, E.A. Dabbish, and R.H. Sloan CHES'99 [15]	
적용	RSA	RSA	RSA	

호에 대한 DPA 공격[13] 중에서 SEMD (single-exponent, multiple data)방법은 이미 알고 있는 키와 스마트카드를 이용하여 미지의 스마트카드 비밀키를 알아내려고 하는 공격 방법이고, MESD (multiple-exponent, single data)는 키의 값을 수정할 수 있는 비교용 스마트카드와 공격대상 스마트카드로부터 멱승 과정에서의 평균 소비전력을 구한 다음 이를 이용하여 각각에 대한 차분 데이터를 계산하여 더 긴 시간 동안 "0"이 나타나는 경우가 올바른 키로 추정하는 공격 방법이다. 그리고 ZEMD (zero-exponent, multiple data)는 하나의 스마트카드에 대하여 특정 바이트의 해밍 중을 분류함수로 지정하여 전력을 두 부류로 분류한 후 DPA 공격을 적용하는 방법이다. 상기 세 가지 공격 중에서는 일반적으로 ZEMD 공격이 가장 강력한 것으로 알려져 있다.

3. DPA 공격 및 대응방안

DPA [8-12]는 비밀키와 정확히 상관관계 (correlation)를 가지는 정보를 추출하기 위해 통계

적인 분석 (statistical analysis)과 에러정정 (error correction) 기술을 사용한다. 즉, 스마트 카드가 암호학적 연산을 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음, 표본화된 데이터를 잡음신호 감소와 차분 (differential) 신호의 명확성을 위해 디지털 신호 해석과 통계적인 방법으로 분석하는 공격 기법이다.

DPA 공격방법은 전력소비 데이터를 수집한 후 이를 분석하기 위하여 통계적인 분석방법을 사용하여야 한다. 먼저 정확한 비밀키가 들어갔을 때 그 비밀키와의 반응을 알 수 있는 분류함수 (partitioning function) 또는 선택함수(selection function)인 $D(key, data)$를 정하여야 하는데, 이 함수는 특정 비트나 바이트의 해밍 중을 조사하여 데이터 수집단계에서 수집한 데이터를 분류하는 함수이다. 이러한 분류함수로 데이터를 적절히 분류한 후 가능한 비밀키의 집합에서 키를 추측하여 통계적인 방법으로 비밀키를 찾아낼 수가 있으며, 다음은 DPA의 전체적인 단계를 나타내었다.

① 전체 구하려는 스마트 카드의 n 비트 비밀키 K를 $(k_{n-1}, k_{n-2}, \cdots, k_1, k_0)$라 정의하고, 최상위 혹은 최하위 비트의 순서로 순차적으로 키의 일부가 입력되어 연산된다고 가정한다.

② 먼저 키의 일부인 k_i 또는 $\{k_i, \cdots, k_j\}$를 미리 가능한 키 영역에서 추측한다.

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

$$S_0=\{S_i[j] \mid D(key, data) = 0 \text{ or low hamming weight}\}$$
$$S_1=\{S_i[j] \mid D(key, data) = 1 \text{ or high hamming weight}\}$$

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-zero이고 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 스마트 카드의 실제 내부 키 일부가 된다.

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

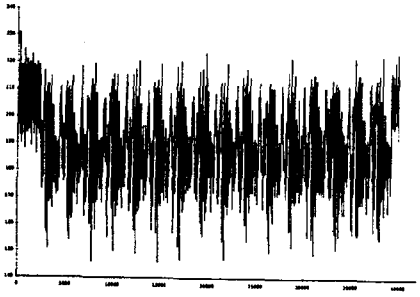


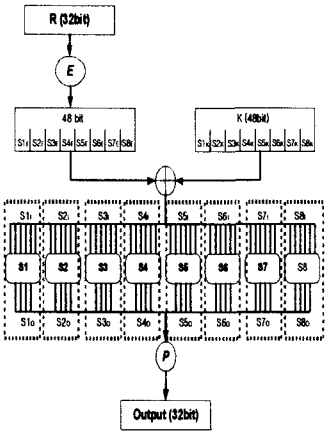
그림 1. 16 라운드 DES 계산에서 측정된 전력 소모 파형

각각 하나의 Δ_{D_i}에 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.

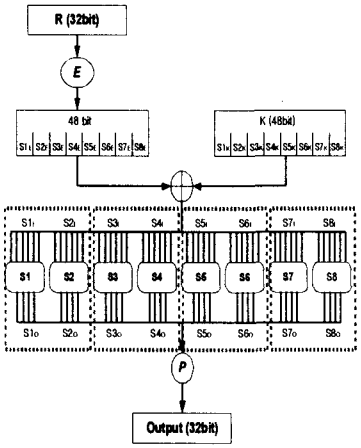
프랑스 불 스마트카드(Bull smartcards)사의 Goubin 등[11-12]이 공격한 DPA 방법은 다음과 같다. 그림 1은 DES 16 라운드 과정을 실제로 측정한 파형이다.

그림 2와 표 4에는 기존 방안과 차별화가 이루어진 소프트웨어적인 소스 코딩 방법을 제안한다. 기존의 방법에서는 a)와 같이 8개의 개별 S-box 단위로 읽어내는 원리이며, 이 경우에는 표 4의 1)방안에서처럼 단계적인 공격에 의하여 2^{17} ($=2^6 \times 8 \times 2^8$; DPA 분석단계에서 첫 번째 6비트를 추정하기 위하여 2^6번의 ②~⑦과정이 필요하고, 이러한 6-비트 블록이 8개를 반복하여야 하며, 마지막으로 나머

지 8비트를 전수 검사하기 위하여 2^8이 필요함) 분석 복잡도를 갖음을 알 수 있고, 결과적으로 DPA 방법에 의한 암호해독이 가능함을 알 수 있다. 하지만 8 개의 S-box를 두 개씩 그룹화하여 구현할 경우인 2)방안에서는 S-box를 두 개씩 한꺼번에 추정하여야 하기 때문에 분석 복잡도가 2^{22} (=2^{6-6} x 4 x 2^8)으로 증가한다.



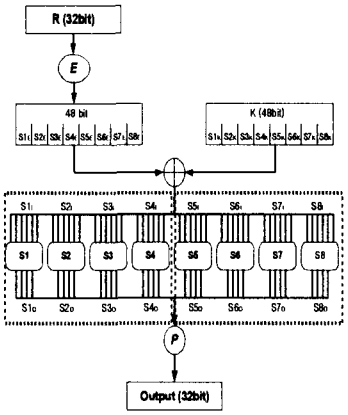
a) 기존 코딩 방법



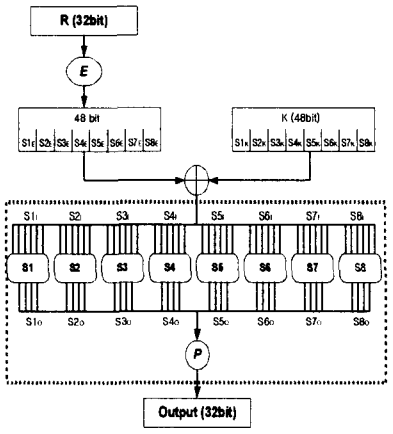
b) 대응 방안-1 (12-bit key guessing)

그림 2. 두 S-box씩 묶어서 구현하는 대응 방안

그림 3과 표 4에는 스마트카드에 소프트웨어 형태로 탑재된 DES-like 알고리즘에 대하여 DPA 공격에 견딜 수 있는 소프트웨어적인 방어대책을 제안하였으며, 그 방법은 S-box를 2개/4개/8개 씩 그룹화하여 그룹단위로 프로세싱(read, write)하도록 코딩하게 된다면 DPA 공격에 대한 강도가 현재 방법보다 강할 수 있음을 보여 주고 있다.



a) 대응 방안-2 (24-bit key guessing)



b) 대응 방안-3 (48-bit key guessing)

그림 3. 네 개 또는 여덟 개의 S-box씩 묶어서 구현하는 대응 방안

특히, DES에 대한 DPA 공격 계산 복잡도는 기

존방법에서 2^{17}, 2개씩 묶어서 프로세싱할 경우에는 2^{22}, 4개씩 묶어서 프로세싱할 경우에는 2^{33}, 마지막으로 8개 단위로 한꺼번에 프로세싱이 될 경우에는 전수공격에서의 계산 복잡도인 2^{56}에 이를 수 있음을 보여주고 있으며, 또한 이 방법은 여러 대의 컴퓨터를 이용한 키 전수공격 방법이 적용되지 않기 때문에 이러한 공격에 안전하다고 할 수 있다.

표 4. DES-like 알고리즘에서 DPA 방어 대책 제안

항목	1) 기존 방안 (6-bit key guessing)	2) 두 개의 S-box씩 묶어서 수행 (12-bit key guessing)	3) 네 개의 S-box씩 묶어서 수행 (24-bit key guessing)	4) 여덟개의 S-box씩 묶어서 수행 (48-bit key guessing)
제안 내용	원래의 방법으로 S-box를 순차적으로 프로그래밍 할 경우이므로 별도의 대책이 요구됨.	인접하는 S-box를 두 개씩 묶어서 프로그래밍 할 경우임.	인접하는 S-box를 네 개씩 묶어서 프로그래밍 할 경우임.	S-box를 모두 묶어서 프로그래밍 또는 하드웨어 구현할 경우임.
S-box 입출력 비트수	Input: 6-bit Output:4-bit # of S-box groups: 8	Input: 12-bit Output: 8-bit # of S-box groups: 4	Input: 24-bit Output: 16-bit # of S-box groups: 2	Input: 48-bit Output: 32-bit # of S-box groups: 1
공격 순서	S1-box → S2-box → S3-box → S4-box → S5-box → S6-box → S7-box → S8-box	S1,S2-box ↓ S3,S4-box ↓ S5,S6-box ↓ S7,S8-box	(S1,S2,S3,S4) ↓ (S5,S6,S7,S8)	(S1,S2,S3,S4, S5,S6,S7,S8)
공격 단계 수	8	4	2	1
분석 복잡도	$[2^{6}x8] \times 2^{(56-48)} = 2^{17}$	$[2^{12}x4] \times 2^{(56-48)} = 2^{22}$	$[2^{24}x2] \times 2^{(56-48)} = 2^{33}$	$[2^{48}x1] \times 2^{(56-48)} = 2^{56}$

4. 결 론

DPA는 SPA 보다 방어하기 더 어려운 강력한 공격방법이며, SPA가 소비 전력을 관찰하는 것에 반하여, DPA는 비밀키와 정확히 상관관계(correlation)를 갖는 정보를 추출하기 위해 통계적인 분석 (statistical analysis)과 에러정정 (error correction) 기술을 사용한다. 본 논문에서는 스마트카드가 암호학적 연산을 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음, 표본화된 데이터를 잡음신호 감소와 차분 (differential) 신호의 명확성을 위해 디지털 신호 해석과 통계적인 방법으로 분석하는 DPA 공격 기법에 대하여 분석하였다.

또한, 스마트카드에 소프트웨어 형태로 탑재된 DES-like 알고리즘에 대한 DPA 공격을 견딜 수 있는 핵심적인 방어대책을 제안하였으며, 제안 방법은 S-box를 2개/4개/8개 씩 그룹화하여 그룹단위로 프로세싱(read, write)하도록 코딩하게 된다면 DPA 공격에 대한 강도가 현재 방법보다 강할 수 있음을 보여주고 있다. 특히, DES에 대한 DPA 공격 계산 복잡도는 기존방법에서 2^{17}, 2개씩 묶어서 프로세싱할 경우에는 2^{22}, 4개씩 묶어서 프로세싱할 경우에는 2^{33}, 마지막으로 8개 단위로 동시에 프로세싱이 될 경우에는 전수공격에서의 계산 복잡도인 2^{56}에 이를 수 있음이 분석됨에 따라 마지막 방법으로 구현할 경우 안전성이 높아지고, 여러 대의 컴퓨터를 조합한 키 전수공격기법이 적용되지 않기 때문에 이러한 방법에 안전하다고 할 수 있다.

References

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

[2] ISO/IEC 10536, Identification Cards-Contact-less Integrated Circuit(s) Cards, ISO Standard.

[3] ISO/IEC 14443, Identification Cards-Remote Coupling Communication Cards, ISO Standard.

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

[5] 박창섭, "암호이론과 보안," 대영사, 1999.

[6] 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.

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

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

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

[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.

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

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

[13] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," CHES'99.

[14] P. Fahn and P. Pearson, "IPA: A new class of power attacks," CHES'99.

[15] T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," CHES'2000, pp.238-251.

[16] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Proceedings of Advances in Cryptology-CRYPTO'96, pp.104-113, Springer-Verlag, 1996.

[17] E. Biham, A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in Proceedings of Advances in Cryptology-CRYPTO'97, pp. 513-525, Springer-Verlag, 1997.

이 훈 재 (Hoon-Jae Lee)
1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)
1987년2월~1998년1월 :국방과학연구소 선임연구원
1998년 2월~2002년 2월 : 경운대학교 컴퓨터전자 정보공학부 조교수
2002년 3월~현재 : 동서대학교 인터넷공학부 정보 네트워크공학전공 조교수
(관심분야 : 정보보호, 네트워크보안, 정보통신)

최 희 봉 (Hee-Bong Choi)
1984년 2월 : 부산대학교 전기공학과 졸업(학사)
1987년 2월 : 부산대학교 전기공학과 졸업(석사)
2002년 8월 : 성균관대학교 전전컴공학부 졸업(박사)
1987년2월~2000년1월:국방과학연구소 선임연구원
2000년 1월~현재 : 한국전자통신연구원 부설 국가 보안기술연구소 선임연구원
(관심분야 : 정보보호, 네트워크보안, 보안시스템 설계)

이 상 곤 (Sang-Gon Lee)
1986년 2월 : 경북대학교 전자공학과 졸업(학사)
1988년 2월 : 경북대학교 대학원 전자공학과 졸업(통신공학, 공학석사)
1993년 2월 : 경북대학교 대학원 전자공학과 졸업(정보통신공학, 공학박사)

1991년3월~1997년2월:창신대학 정보통신과 조교수
1997년 3월~현재:동서대학교 인터넷공학부 정보네트워크공학전공 조교수
(관심분야 : 암호이론, 네트워크보안, 시스템 보안, 부호기술, Java 기술)