전력분석공격에 대한 실험 및 하드웨어적 대응방법의 동향

안만기*, 이훈재**, 황운희*

*국방품질관리소, **동서대학교 인터넷공학부

A Tendency of Experiments and Hardware Countermeasure on Power Analysis Attacks

ManKi Ahn*, HoonJae Lee**, UnHee Hwang*

*Defense Quality Assurance Agency

**School of Internet Engineering, Dongseo Univ.

요 약

스마트카드는 내부의 암호 알고리듬이 수행될 때, 비밀키와 관련된 여러 가지 물리적인 정보가 누출될 가능성이 있다. 이러한 물리적 정보를 이용하는 전력분석공격은 현재 많은 이론적 분석, 실험 및 대응방법이 연구되어지고 있다. 본 논문에서는 국내외 하드웨어적인 전력분석공격 실험 및 대응방법에 대한 최신 연구동향을 분석하고자 한다. 연산과정과 데이터의 해밍 웨이트에 따른 실험 동향을 예측한 후 하드웨어 대응방법들에 대한 동향과 문제점들을 기술한다.

I. 서론

스마트카드는 마이크로 프로세서와 메모리를 내장하고 데이터 연산 처리 기능과 저장 기능을 가진다. 그러나 암호 알고리듬을 구현할 때 고려되지 못한 부가 정보의 누출에 의하여 부-채널공격(side-channel attack)의 대상이 될 수 있다. 특히, 전력분석 공격은 스마트카드에 물리적 변환을 가하지 않고 직접 소모전력 신호의 특성을 파악하여 비밀키를 알아내는 공격방법이다.

Kocher[1]에 의하여 DES에 대한 차분전력공격이 처음 적용된 후, 현재까지 많은 실험과 대응방법이 제시되었다. 그러나 국내에서는 대부분 소프트웨어적인 대응방법에 치중되며, 실험분석에서도 하드웨어적인 실험이 미흡한 상태이다. 이는 공개키 뿐만 아니라 관용키에 대해서도 마찬가지다.

본 논문에서는 국내외 하드웨어적인 전력분석공격 실험 및 대응에 대한 최신 연구동향을 분석하고자 한다. 앞으로의 대응방법에 대한 흐름은 소프트웨어 및 하드웨어적인 방법을 모두 사용할 것으로 예측되며, 국내에서는 소프트웨어적인 대응방법이 주된 연구대상이다.

II. 전력분석 공격 실험의 동향

전력분석 공격의 실험은 실험 기자재의 성능과 공격자의 다양한 실험적 지식 및 스마트카드에 대한 지식을 가지고 있어야 한다. 최근에는 전력분석 공격의 효율성을 높이기 위한 공격 툴이 개발되어지고 있다. *Crypto Research*는 CRI's DPA testing tool을 선보여 14.5만달러에서 20만 달러정도의 구입 비용이 소요됨을 보였다[2]. 또한 Eindhoven 대학에서는 소프트웨어는 물론 하드웨어도 테스트 할 수 있는 "PINPAS" 프로그램을 소개하였다. 이러한 공격에 대해 저자는 대응방법으로 Dual-rail logic이 효과적임을 언급하였다.[3] 그 외에도 *Graz* 대학에서는 하드웨어적인 대응방법과 공격 툴을 개발하고자 프로젝트를 수행중이다.

1. 알고리듬 연산과정에 대한 실험

국외에서는 Messerges [4]의 실험을 시작으로

다수의 실험 결과가 발표된 바 있다. 국내에서도 상용 스마트카드에 암호알고리듬을 내장시키고 실험을 실시하는 형태를 취하고 있다. 스마트카드에 공개키 알고리듬을 내장시키고 비밀키에 따른 연산 과정의 차이로 소모전력을 차분하는 실험을 성공하였다[5]. 이는 클럭 단위로 해밍웨이트의 소모전력을 측정하지 않고 비밀키에 따른 연산과정의 상이함을 이용한 실험방법이다. 또한 소프트웨어 대응방법도 제안된 바 있다. [6,7]

2. 데이터의 해밍웨이트에 따른 실험

Kocher [1]가 DES에 차분전력 공격을 처음으로 적용하였다. 데이터의 '0'과 '1'에 따른 소모전력 차이를 이용한 방법으로 해밍웨이트에 의한 실험은 클럭 단위의 정밀함과 고정밀의 트리거가 필요하며 샘플 할 소모전력 데이터도 상당히 증가한다. 최근 국내에서 Self-timed effect를 DES 및 AES알고리듬에 적용하여 실험 결과가 발표되었다[8]. 또한 일부 스마트카드 제조회사에서는 암호알고리듬에 대한 칩 안전성을 연구하고 있다. 국외에서는 해밍웨이트 이론을 기반으로 직접 FPGA 적용 실험을 실시하고 있다. DES 알고리듬을 PIC 16F84A microcontroller와 VHDL을 사용한 Xilinx FPGA에서 실험이 실시되고 있으며, TU Graz 대학과 COSIC 연구그룹에서는 8051 micocontroller와 Xilinx Virtex FPGA를 이용하여 DES와 공개키 알고리듬에 대한 소모전력을 실험하고 Matlab을 이용하여 AES를 시뮬레이션을 하였다. 이는 소프트웨어적인 실험이 아닌 암호시스템을 하드웨어적으로 구현한 모델을 적용한 실험이었다.[9,10,11,12,13,14] 또한 G3CARD 컨소시엄에서는 스마트카드에 비동기 회로(Asynchronous logic)의 적합성을 연구하여 현재까지 다양한 실험을 실시하고 있다. [15] 이러한 실험과 함께 최근, Roman Novak은 신호기반 전력분석(Sign-based DPA)을 이용하여 관용키 알고리듬을 역설계(reverse engineering)하는 기법을 발표하였다. 이는 해밍웨이트에 따른 소모전력을 기반으로 비밀스런 암호 알고리듬의 내부를 추적하는 방법으로 전력분석공격으로 키뿐만 아니라 암호 알고리듬 코드도 추적할 수 있다는 것이다. [16]

Ⅲ. 하드웨어 대응방법의 동향

전력분석 공격의 대응방법으로 크게 두 가지로 분류된다. 비밀키에 따른 연산과정을 동일하게 실시하도록 암호알고리듬을 재구성하는 소프트웨어 대응방법과 고접적회로 설계 단계에서 데이터 비트의 소모전력을 유사하게 조절하는 하드웨어 대응방법이 있다. 최근에는 소프트웨어 대응방법이 더 활발이 연구되고 있으나, 하드웨어적인 방법과 병행하는 것이 더욱 안전하다고 발표되고 있다. 국내에서는 공개키 알고리듬에 랜덤성을 이용한 소프트웨어 대응방법이 주로 연구되어지고 있다. [6,7] 본 절에서는 국외의 하드웨어 대응방법의 동향을 간략히 기술한다.

1. Self-timed dual-rail method 구현

소모동작전력을 균등화하는 비동기 이중선로 방식(Self-timed dual-rail method)은 데이터 한 비트를 두개의 선로를 이용하여 나타내는 코딩방법이다. 데이터 값 '1'은 '10'으로 '0'은 '01'로 인코딩되어 유효한 데이터의 도착을 전역클럭 신호 없이도 찾을 수 있다. 이러한 코딩 방법은 암호화 연산 수행 시 데이터 비트 값에 따른 같은 개수의 데이터 천이(data transition)가 발생하여 소모전력의 차이를 최소화 할 수 있다. 또한 비동기 회로는 각각의 회로들이 전역 클록신호에 따라 동작하지 않아 각 연산들의 동작 시점이 달라 실험에 있어 동기화를 힘들게 한다. ACiD 연구그룹과 Cambridge 대학 그리고 Gemplus사는 스마트카드 안전성과 self-timed microcontroller에 대한 연구를 실시하여 1-of-n data encoded SI circuit를 구현하였다. Amulet 그룹에서는 ARM 호환 microprocessor로 스마트카드의 회로설계에 적용하였다.[8,15,17,18] 그러나 최근에는 이러한 dual-rail method나 부가적인 logic을 사용하여도 대응방법으로는 충분하지 않다고 연구되고 있다. 이것은 칩 버스(Bus)들의 인접한 라인에서 신호 변환이 일어나 소모전력 차이가 발생하는 것이 원인이라고 한다. [19]

2. Sense Amplifer Based Logic 구현

회로 설계 단계의 대응방법으로 차동 논리(differential logic)와 동적 논리(dynamic logic)의 조합으로 신호의 변화와 소모전력이 독립적으로 이루어지도록 구현한다. 차동 논리에서는 공격자가 0-1/1-0 천이와 0-0/1-1 천이 중에서 전력을 많이 소모하는 0-1/1-0 천이를 구별할 수 있다. 그리고 동적 논리에서는 0-1/1-1 천이와 0-0/1-0 천이 중에서 전력을 많이 소모하는 0-1/1-1 천이를 구별할 수 있다. 이러한 천이 과정에서 클럭에 따른 충방전 시에 항상 일정한 값을 유지하는 커패시턴스를 사용하여 입력에 무관한 출력을 생성하는 sense amplifer 기술로 4가지의 상태천이를 구별할 수 없도록 구현 가능하다. 그러나 전력변화율이 기존에 비해 116배 감소한 반면 면적과 소

모전력이 2배로 증가하며 차동 논리에서는 사전에 충전해야 할 소자를 가지고 있어야한다. 또한 종속회로(Cascade circuit) 구현 문제점이 언급되었다. [20]

3. Decorrelation circuit 구현

FPGA의 조합논리회로(combinational logic block,CBL)의 출력으로 사용되는 플립플롭(flip-flop)에 대하여 출력과 입력의 상관관계가 없도록 구현하는 방법이다. 부가적인 플립플롭을 설계하여 두 플립플롭이 서로 다른 상태를 가지고 있어서 클럭에 따른 천이의 합이 항상 일정하게 유지되도록 설계하는 것이다. 따라서 각 출력 커패시턴스의 전압이 비슷하게 유지될 수 있다. 이런 구조는 비밀키와 원래의 플립플롭간의 상관관계를 줄인다. XNOR gate를 추가하여 설계하였다. 그러나 성능 측면에서 적용된 CBL가 FPGA 전체 면적의 9.63%에 이르기 때문에 큰 효과를 얻을 수 없고, 회로상의 글리치(Glitch) 문제도 고려해야 한다. [12]

4. Non-deterministic processor구현

명령어 체계를 변형함으로서 데이터와 소모전력 파형간의 상관관계(correlation)을 제거하여 동기화가 실패하도록 로직을 구성한다. 기존의 fetch, decode, execute, write 과정을 순차적으로 실행하는 CISC 구조가 아닌 각각의 과정이 단계적으로 겹쳐서 실행되는 RISC 구조에 적용되며, 이 때 임의의 실행구간에 랜덤한 Break time 구간을 삽입하는 방법이다. 명령어의 사용 레지스터를 랜덤하게 재명명하는 복잡한 소프트웨어 구현 방법보다는 microcontroller의 decoding 명령들을 하드웨어적인 모듈로 구성하여 실행하도록 제안하였다. [21]

5. Power masking method 구현

5단계의 실행 과정(fetch, decode, execute, memory access, write)을 가지는 32비트 내장형 프로세서를 이용하여 load operation 단계를 변형하는 방법이 제안되었다. 데이터가 이동하는 기존의 버스에 32비트 부가적인 버스를 추가하여 64비트 버스로 구성한다. 이때 64비트 버스는 사전에 '1'로 충전되고 실행 과정에서 커패시턴스를 통해 32비트 버스의 부가적인 비트에 해당하는 전력을 방전시킨다. 즉, 입력 데이터와 무관한 데이터 버스가 소모전력을 일으킨다. 변형된 구조를 DES에 적용하여 효과적임을 검증하였으나 구현상에 잉여 커패시턴스가 필요하다.[19] 또한 랜덤 클럭 게이트와 전력 관리 기술으로 추가적인 소모전력을 증가시키지 않으면서 Power-managed unit를 구현하고 RSA 알고리듬을 대상으로 실험하였다. 이때 랜덤수 생성기는 선형 궤환 쉬프트 레지스터(linear feedback shift register, LFSR)로 구현하였다. [22]

6. Custom logic block 구현

칩 제조사는 부-채널공격에 대응하기 위한 다양한 방법을 구현하고 있다. 칩 설계 시 Custom Logic Block을 만들어 데이터가 CPU의 입출력 전에 통과하도록 설계하였다. 이는 공격자가 내부 동작을 분석하지 못하도록 설계하는 것이다. [23] 또한 커패시터의 방전시간을 이용하는 ant-DPA 블록을 설계하여 소모전력 분석 시간을 늘리는 대응방법도 제안되었다. [24]

7. 기타

하드웨어 대응방법으로 스마트카드 제조 과정에서 랜덤 클럭 지터링을 가지는 내부 클럭 생성기나 부가적인 dummy 명령어, 사이클, 언터럽트, 노이즈, 물리적 shielding 등을 추가하는 방법이 제안되었다. [25] 그 외에도 다양한 설계기법을 적용하여 소모전력량을 제한하거나 줄이기 위한 노력을 하고 있다.

IV. 하드웨어 대응방법의 문제점

하드웨어 대응방법의 가장 단순한 아이디어는 데이터에 따른 소모전력을 독립적으로 구현하는 것이다. 즉, 플립플롭(flip-folps)의 출력을 입력에 관계없이 동일하게 하는 것인데 이때 구현되는 게이트의 수가 증가하여 비용과 소모전력이 상승되고, 칩 집적도가 증가된다. 예를 들어 Balanced self-checking asynchronous logic은 면적이 3배 정도 증가되며, 처리 속도도 느리게 된다. 그러나 이러한 문제점은 앞으로의 고접적 설계 기술이 향상될 때 극복될 수 있으리라 믿는다. 그 외에도 다른 물리적 공격(시차공격, 오류공격, 전자기 누출공격)에 모두 대응할 수 없다는 점이다. 따라서 안전성 측면이 우선적으로 고려된 새로운 설계방법이 개발되어야 한다. 표1에서는 위의 대응방법에 대한 문제점들을 간략히 요약하였다.

V. Future Work

전력분석 공격의 대응방법은 하드웨어 대응 및 소프트웨어 대응방법을 모두 사용하는 것이 유리하다. 현재로서는 각각의 대응방법을 별개로 적용하는 추세이다. 그러나 앞으로는 알고리듬을 재구성하고 최소한의 소모전력을 가지는 커패시터와 부가적인 소자를 사용함으로써 전력분석 공격뿐만

표 1 : 대응방법의 문제점

대응방법	문제점	실험대상	Ref.
Self-timed dual-rail method	인접라인에 의한 소모전력의 영향	RSA, CMOS logic	[8] [15] [17] [18]
Sense amplifer based logic	면적과 소모전력 증가, 사전 충전	CMOS logic	[20]
Decorrelation circuit	면적 증가, 글리치 현상	FPGA simulation	[12]
Non-deterministic processor	RISC 구조에만 적용	-	[21]
Power masking method	소모전력 증가, 부가적인 커패셔터 사용	DES, RSA	[19]
Custom logic block	커패셔터의 성능, 범용성	CMOS logic, FPGA	[23] [24]

아니라 기타 다른 부-채널공격의 대응방법으로 구현되어야 할 것이다. 또한 커패시터에 의존하는 대응방법이 아닌 Non-deterministic processor 방법과 연산과정의 랜덤성 그리고 비동기회로 등을 하드웨어적으로 조합한 효과적인 대응방법도 구현해야 할 것이다. 마지막으로 기존의 대응방법들을 동일한 조건에서 비교 평가하는 연구가 이루어져 더욱 안전한 대응방법을 설계해야 할 것이다.

VI. 결 론

본 논문에서는 현재 활발히 연구되고 있는 전력분석공격에 대하여 하드웨어적인 실험 및 대응방법의 최신 동향을 분석하였다. 국내외의 연구 동향을 분석하였으며, 이에 대한 문제점을 간략히 기술하였다. 국외에서는 많은 연구기관과 학계에서 다양한 대응방법을 제시하고 있으나, 국내에서는 하드웨어 대응방법에 대한 인식이 미흡한 점이 있다. 국내외의 하드웨어 대응방법의 흐름을 파악함으로써 향후 전력분석 공격에 대한 소프트웨어 및 하드웨어 대응방법의 연구에 도움이 될 것이다.

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *CRYPTO'99*, pp. 388-397, 1999.

[2] Patrick Corman and David Finkelstein, " Cryptography Research Introduces Tool to Help Make Smart Cards Safer New DPA Workstation Cuts Time, Cost to Test for Smart Card Leaks", available to http://www.smartcardauthority.com/12_11_02news.html, 2002

[3] J. den Hartog 외 4, "PINPAS : a tool for power analysis of smartcards", in SEC 2003, IFIP WG 11.2 Small Systems Security, pp. 447-451, 2003

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks on Moular Exponentiation in Smart cards", in *CHES'99*, pp. 144-157, 1999.

[5] 안만기, 이훈재, 하재철, 김동렬, 문상재, "스마트카드의 MESD공격에 대한 실험적 분석", 경북대 전자기술연구지, Vol 23, pp. 1-7, June, 2003

[6] MahnKi Ahn 외 3, "A random M-ary method-based Countermeasure against Power Analysis Attacks on ECC", in ICCSA'03, LNCS 2668, Springer-Verlag, pp. 18-21, 2003

[7] JaeCheol Ha and SangJae Moon, "Randomized signed-scalar multiplication of ECC to resist power attacks," in *CHES'02*, LNCS 2523, Springer-Verlag, pp.553-565, 2002.

[8] 이동욱, 이동익, "비동기회로 설계기술을 이용한 DPA(차분전력분석공격) 방어방법에 관한 연구", 대한전자공학회 하계학술대회, 2003.

[9] Larry T. MaDaniel III, " An Investigation of Differential Power Analysis Attacks on FPGA-based encryption Systems", available to scholar.lib.vt.edu/theses/available/etd-06062003-163826/unrestricted/Larry_McDaniel.pdf, Master of Science in Electrical Engineering, May, 2003

[10] Ryan Junee, "POWER ANALYSIS ATTACKS :: A Weakness in Cryptographic Smart Cards and Microprocessors", Bachelor of Computer Engineering & Bachelor of Commerce, November, 2002

[11] Elisabeth Oswald, "On Side-Channel Attacks and the Application of Algorithmic Countermeasures", A PhD Thesis in Graz University of Technology, IAIK, May, 2003

[12] Stefan Mangard, " Calculation and simulation of the Susceptibility of

Cryptographic Devices to Power-Analysis Attacks", A Diploma Thesis, in Graz University of Technology, IAIK, 2003
[13] Siddika Berna Ors, Elisabeth Oswald and Bart Preneel, " Power-Analysis Attacks on an FPGA-First Experimental Results", in CHES 2003, LNCS 2779, Springer-Verlag, pp. 35-50. 2003
[14] Thomas Wollinger and Christof Paar, "How Secure Are FPGAs in Cryptographic Applications(Long version)", Report 2003 /119, IACR, 2003. http://eprint.iacr.org
[15] IST-1999-13515, "Public Final Report", G2 CARD, 2003
[16] Roman Novak,"Side-Channel Based Reverse Engineering of Secret Algorithms" In the 12th International Electrotechnical and Computer Science Conference(ERK 2003). pp. 445-448, 2003
[17] L.A. Plana 외 5, "SPA- a Synthesisable Amulet Core for Smartcard Applications", in the Eighth International Symposium on Asynchronous Circuits and Systems (ASYNC 2002). pp. 201-210, 2002
[18] Simon Moore, Ross Anderson, Robert Mullins and George Taylor, "Balanced self-checking asynchronous logic for smart card applications" in the Microprocessors and Microsystems Journal in 2003
[19] H. Saputra 외 5, " Masking the energy behavior of DES encryption", DATE 2003
[20] K. Tiri, M. Akmal and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart card", in The preliminary conference program, *ESSCIRC 2002*, available on Web site http://ele.unipv.it/esscirc2002/
[21] Feyt, "Countermeasure method for a microcontroller based on a pipeline architecture", US PATENT 20030115478 A1, 2003
[22] U. Benini 외 5, "Energy-aware design techniques for differential power analysis protection", in the 40th conference on Design automation(DAC 2003), pp. 36-41, 2003
[23] Hurgen Bohler, "Advanced security functions for smart card chips", STMicroelectronics, Grasbrunn, in GMD-SmartCard Workshop, Session V, 2001
[24] Marinet et al., "Method and device for protecting integrated circuit against piracy", US PATENT 20020124183 A1, 2002
[25] J.F Dhem and N. Feyt, "Hardware and Software Symbiosis Helps SmartCard Evolution", IEEE Micro 21, pp. 14-25, 2001