비동기회로 설계기술을 이용한 DPA(차분전력분석공격) 방어방법에 관한 연구

이 동 욱, 이 동 익
광주과학기술원 정보통신공학과
전화 : 062-970-2248 / 핸드폰 : 017-267-0683

Study on DPA countermeasure method using self-timed circuit techniques

Dong-Wook Lee, Dong-Ik Lee
Dept. of Info. & Comm. Kwang-Ju Institute of Science and Technology
E-mail : dwlee@kjist.ac.kr, dilee@kjist.ac.kr

Abstract

Differential Power Analysis(DPA) is powerful attack method for smart card. Self-timed circuit has several advantages resisting to DPA. In that reason, DPA countermeasure using self-timed circuit is thought as one of good solution for DPA prevention.
In this paper, we examine what self-timed features are good against DPA, and how much we can get benefit from it. Also we test several self-timed circuit implementation style in order to compare DPA resistance factor.
Simulation results show that self-timed circuit is more resistant to DPA than conventional synchronous circuit, and can be used for designing cryptographic hardware for smart-card.

I. 서론

최근 스마트카드의 사용이 급격히 증가함에 따라 스마트카드에 대한 다양한 공격방법들 또한 급속히 발전하고 있다. 이러한 다양한 공격방법 중, 차분전력분석공격(Differential Power Analysis)은 스마트카드에 대한 가장 강력한 공격들 중의 하나로 여겨지고 있으며, 많은 연구들을 통해 이러한 공격을 차단하려는 시도들이 이루어지고 있다. 최근 비동기회로(Self-Timed circuit) 설계기술을 이용한 차단방법 개발에 관한 연구들이 활발히 진행되고 있으며, 첫 번째 프로토타입 칩[2]도 이미 개발되었다. 그러나 비동기회로설계기술을 이용한 차분전력분석공격 차단방법은 대부분 동작전력 균등화(Operation Balancing)에 초점이 맞추어 진행되어 왔다. 본 논문에서는 동작전력균등화 이외의 비동기회로 특성들이 차분전력분석공격 방어에 미치는 영향과 각각의 영향에 대한 Powermill™ 시뮬레이션을 수행하였다.

II. 차분전력분석공격(DPA)

2.1 전력분석공격(Power Analysis)

전력분석공격이란 칩으로 구현된 스마트카드의 암호화 하드웨어의 동작 중에 소모되는 전력패턴을 관찰하여, 비밀키와 같은 내부의 보안정보를 찾아내어 해킹하는 공격방법이다. 전력분석공격은 칩 내부의 연산과정에서 소모되는 전력이 연산되는 데이터 값과 상호연관성(Correlation)을 갖는다는 사실에 기초한다. 그러나 최근의 암호화 하드웨어들은 적은 전력소비량과 빠른 동작속도를 갖기 때문에, 단순한 전력소모패턴의 관찰을 통해서는 이러한 공격을 수행하는 것이 점차 어려워지게 되었다. 이를 극복하기 위해 새로운 공격방법인 차분전력분석공격방법이 개발되었다.

2.2 차분전력분석공격(DPA)

차분전력분석공격은 단순전력분석을 통해 알아낼 수

없는 미세한 전력패턴과 데이터간의 상관관계를 찾아내는 공격방법이며, 다음과 같이 정의된다.

$$DPA[j] = A_0[j] - A_1[j] \quad (1)$$

여기에서, $A_0[j]$와 $A_1[j]$는 다음과 같다.

$$A_0[j] = \frac{1}{|S_0|} \sum_{S_i[j] \in S_0} S_i[j]$$
$$A_1[j] = \frac{1}{|S_1|} \sum_{S_i[j] \in S_1} S_i[j] \quad (2)$$

$$S_0 = \{S_i[j] | D() = 0\}, S_1 = \{S_i[j] | D() = 1\} \quad (3)$$

$S_j[i]$: i 번째 입력의 연산시 관찰된 전력소비패턴

$D(x, y, z...)$: DPA 분류 함수 (DPA Classification Function)

많은 입력 값들의 전력신호를 평균함으로써, 측정오차에 의한 잡음과 관찰하고자 하는 데이터부분과 관련이 없는 부분에 의한 잡음을 제거하게 되며, 결과적으로 최종 DPA 결과 신호에서는 원하는 부분만의 전력소모를 관찰할 수 있게 된다.

III. 비동기회로 설계 기법을 이용한 차분전력분석공격 차단방법

비동기 회로는 잠재적으로 다음의 두 가지 특성에 의해 차분전력분석 공격차단에 유리하다.

① 특수한 비동기 데이터 인코딩 방법에 의한 동작전력균등화(Operation Balancing)

② 전역클록신호(Global Clock Signal)의 부재로 인한 DPA 동기실패(DPA Synchronization Failure)

3.1 동작전력균등화(Operation Balancing)

비동기 회로는 기존의 동기식 회로와는 다른 다양한 데이터 인코딩 방법을 사용하고 있다. 표1은 다양한 데이터표기방법들 중 대표적인 이중선로 데이터 인코딩을 보여주고 있다. 유효한 데이터전송 사이에 "00"이라는 Spacer신호로 초기화를 시켜주게 되며, 데이터0을 전송시 "01"을 데이터1을 전송시 "10"을 인가하여 유효한 데이터의 도착을 전역클록신호 없이도 찾을 수 있게 된다. 이러한 데이터 인코딩은 전송하는 데이터 값에 무관하게, 언제나 같은 개수의 데이터 천이(Data Transition)가 발생하게 되며, 따라서 암호화 하드웨어를 설계하면, 입력데이터 1과 0을 처리할 때 나타나는 전력소모 패턴의 차이를 최소화 할 수 있다. 식 1에서와 같이 차분전력분석공격은 기본적으로 데이터1과 데이터 0을 처리할 때 발생하는 전력소모패턴의 차이를 이용하여 해킹 하게 되므로, 이러한 데이터코딩을 사용할 경우 차분전력분석공격을 더욱 어렵게 할 수 있다.

Spacer	00
Data 0	01
Data 1	10

표 5 Self-Timed Dual-Rail Encoding Method

그림 1은 범용 표준 게이트들을 이용하여 이중선로 방식의 비동기 XOR게이트를 설계한 회로이며, 그림 2는 비동기 C-ELEMENT회로를 사용하여 이중선로방식의 비동기 XOR게이트를 구성한 회로이다.

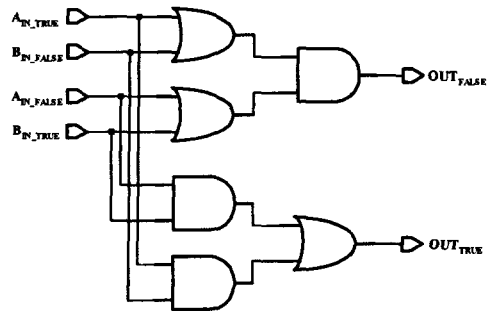

그림 1 범용 게이트 셀을 이용한 비동기 이중선로 방식의 XOR게이트

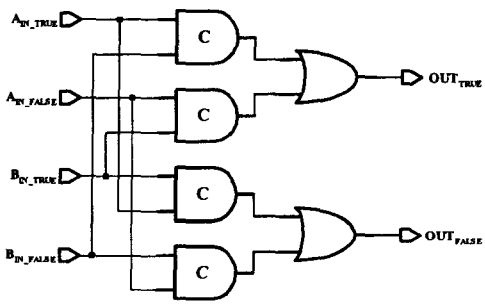

그림 2 비동기 C-ELEMENT 셀을 이용한 비동기 이중선로 방식의 XOR게이트

두회로 모두 1개의 데이터입력값에 대해 2개의 선로를 가지며, 어떠한 입력데이터 조합을 연산하여도 같은 개수의 데이터 천이개수를 갖는다.

3.2 DPA 동기 실패(DPA Synchronization Failure)

식2와 같이 DPA공격을 수행하기 위해서는 획득한 많은 개수의 전력소모패턴들을 평균하는 작업을 수행

하게 된다. 이러한 평균연산은 공격하고자 하는 전력 소모패턴부분과 상관관계가 없는 부분의 전력소모패턴이나 측정과정에서의 오차 같은 부분을 제거하기 위한 연산과정이다. 이는 공격대상이 되는 연산부분이 전력 소모패턴그래프에서 언제나 시간축상에서 비슷한 위치에 존재한다는 가정 하에 이루어진다.

이 과정에서 시간축상에서 동기가 어긋난 신호들은 전체 공격과정에서 오차로 간주된다. 기존의 동기식 회로에 대한 차분전력분석공격 방법은 전역클록신호를 트리거(Trigger) 신호로 하여 많은 개수의 샘플들을 중첩시켜 통계연산을 수행하도록 하며, 이 과정에서 이러한 동기실패에 의한 오차는 무시될 수 있다. 그러나 비동기회로는 전역클록을 사용하지 않으며, 극단적으로 각각의 게이트들은 자신들의 타이밍으로(Self-timed) 동작하게 된다. 이로 인해 내부적으로 각각의 연산은 시간축상에서 동일한 위치에서 수행되지 않으며, 시간축 상에서의 각 연산들의 위치는 연속적인 분포를 갖게 된다. 따라서 비동기회로로 인해 발생하는 이러한 동기실패오차는 차분전력분석공격을 위해 더 많은 개수의 입력샘플을 요구하게되며, 결과적으로 공격을 더욱 어렵게 한다.

Ⅳ. 실험결과

4.1 XOR 게이트 구현에 대한 실험결과

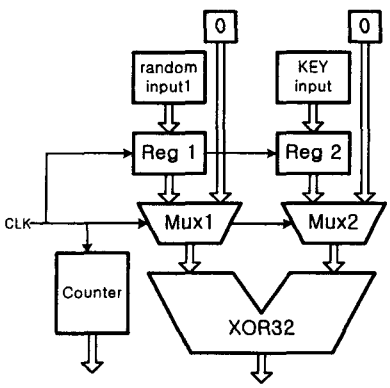

그림 3 XOR게이트에 대한 DPA 공격실험환경

XOR 연산은 암호화 알고리즘의 구현에서 가장 많이 사용되는 연산 중에 하나로, 대표적으로 비밀키와의 연산을 통해 입력데이터의 백색화(whitening)에 사용된다. XOR게이트에 대한 실험은 그림 3과 같이 32비트의 XOR게이트에 대해, 많은 개수의 랜덤 입력과 비밀키와의 XOR연산을 수행시킨 후 각각의 연산에 소모된 전력소모패턴을 획득한 후, DPA통계연산을 통해 입력데이터와 전력소모패턴만을 이용하여 비밀키의 각 비트가 어떤 값인지를 찾아내는 공격을 수행하였다.

그림 4는 기존의 동기식 XOR게이트에 대한 공격실험 결과이다. 적은 개수의 랜덤 입력에 대해서 비교적 뚜렷한 파형의 차이를 얻을 수 있으며, 32비트에 해당하는 비밀키 정보를 모두 획득 가능했다.

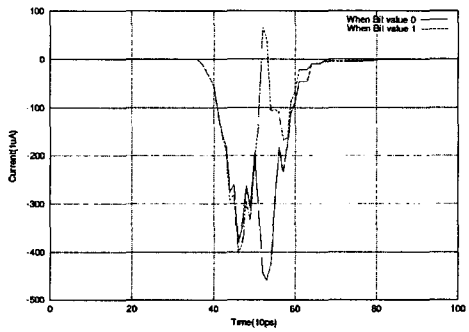

그림 4 동기식 XOR게이트에 대한 DPA공격실험결과(6,000 입력데이터 통계처리)

그림 5는 비동기식 XOR게이트 구현에 대한 실험결과이며, 동기식 회로에 비해 상대적으로 많은 개수의 입력을 인가하여 공격에 성공할 수 있었다.

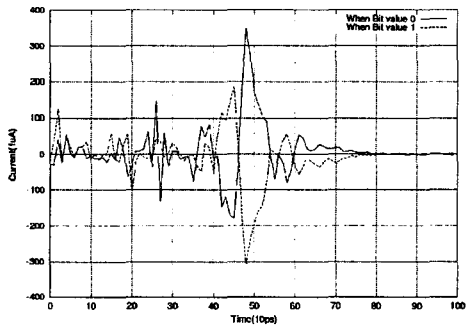

그림 5 비동기식 XOR게이트에 대한 DPA공격실험결과(30,000 입력데이터 통계처리)

그림 6은 비동기식 게이트구현과 비동기식 데이터전송 메커니즘을 함께 사용하여, DPA 통계연산시 시간축상에서의 동기화를 방해한 XOR게이트 회로에 대한 시뮬레이션 결과이다. 실험에서 인가 가능한 최대한의 입력개수에 대해서도 뚜렷한 파형의 차이를 발견할 수 없었으며, 결과적으로 KEY비트의 획득에 실패하였다.

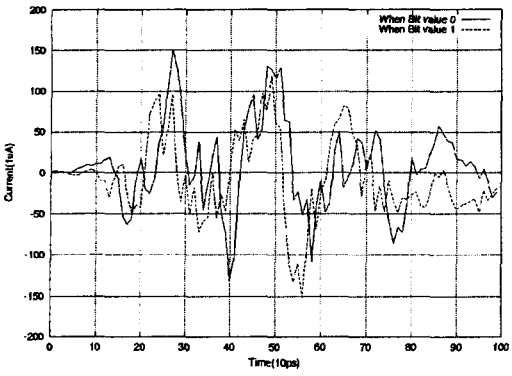

그림 6 비동기식 XOR게이트와 DPA동기실패 매커니즘을 탑재한 XOR게이트에 대한 DPA공격실험결과(65,536 입력데이터 통계처리)

4.2 DES Algorithm 에 대한 실험결과

실제 암호화 회로에 대한 비교실험을 위해, DES알고리즘의 하드웨어 구현에 대한 공격실험을 수행하였다. 각각 그림 7은 동기식으로 설계된 DES알고리즘의 한 라운드에 대한 공격실험결과이다. 올바른 키 값을 추측시 DPA결과신호에서 특징을 발견할 수 있으며, 최종적으로 라운드 키값의 획득에 성공하였다.

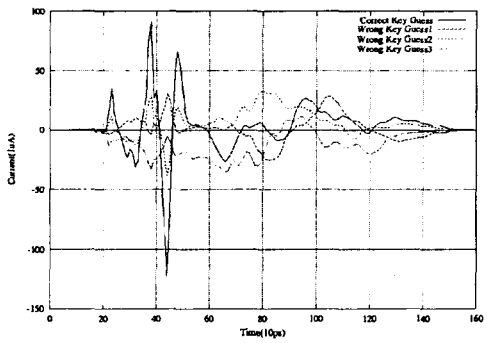

그림 7 동기식 DES 회로의 one round에 대한 차분전력분석공격 실험결과

그림 8은 비동기식으로 설계된 DES알고리즘에 대한 차분전력분석 공격실험결과이며, 올바른 키값을 추측한 것과 틀린 키값을 추측했을때의 파형의 차이를 발견할 수 없었다.

V. 결론

스마트카드의 안전한 사용을 보장하기 위해서는 스마트카드에 대한 차분전력분석공격을 차단하는 방법에 관한 연구와 이를 이용한 하드웨어 설계가 필수적으로 요구되고 있다.

본 논문은 차분전력분석공격을 방어하기 위한 방법의 하나로 비동기회로설계기술이 사용될 수 있음을 보였고, 비동기회로의 각각 어떠한 특성들이 차분전력분석공격의 방어에 사용될 수 있는지를 보였다. 같은 기능을 수행하는 동기회로와의 비교실험 및 다양한 비동기식 설계방법들과의 상호비교를 통해 기존의 회로에 비해 어느 정도의 안전성을 갖는지를 보였다.

본 논문의 결과는 향후 스마트카드를 위한 암호화 코어 설계시, 차분전력분석공격을 방어하기 위한 설계방법선택의 기초자료로 사용될 수 있을 것으로 사료된다

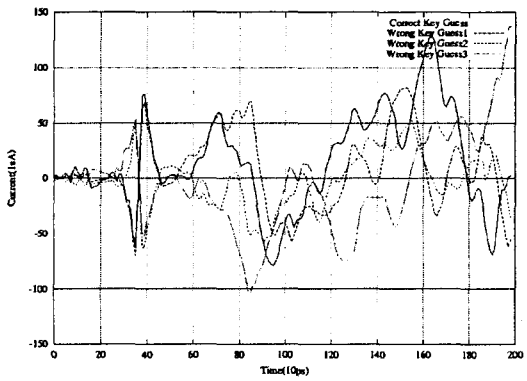

그림 8 비동기식 DES에 대한 one round 차분전력분석공격 실험 결과

Acknowledgement

본 연구는 산업자원부 ELECTRO-0580사업 및 교육인적자원부 BK21 사업에 의한 지원으로 수행되었음

참고문헌

[1] P.C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis,," in Proc. 19th International Advances in Cryptology Conference - CRYPTO'99,, pp. 388-397, 1999.

[2] S. Moore, R. Anderson, P. Cunningham, R. Mullins, G. Taylor, "Improving Smart Card Security using self-timed Circuits,," in Proc. of Eighth International Symposium on Advanced Research in Asynchronous Circuits and Systems,, pp. 211-218, 2002.

[3] C. Clavier, J. Coron, and N. Babbous, "Differential Power Analysis in the Presence of Hardware Countermeasures,," in Proc. of Workshop on Cryptographic Hardware and Embedded Systems(CHES), pp.252-263, 2000.

[4] T. Messerges, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," in IEEE Transactions of Computers, VOL51, NO5, pp. 541-552., May 2002