(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0046417
(43) 공개일자 2010년05월07일

(51) Int. Cl.
G06K 19/073 (2006.01) *G06K 19/07* (2006.01)
G06F 21/00 (2006.01)
(21) 출원번호 10-2008-0105247
(22) 출원일자 2008년10월27일
심사청구일자 2008년10월27일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
정성우
서울 용산구 이촌1동 한가람아파트 217-1002
장형범
서울특별시 송파구 문정2동 훼미리아파트 304-801
이종성
경기 의정부시 호원1동 우성아파트 201동 206호
(74) 대리인
조영현, 나승택

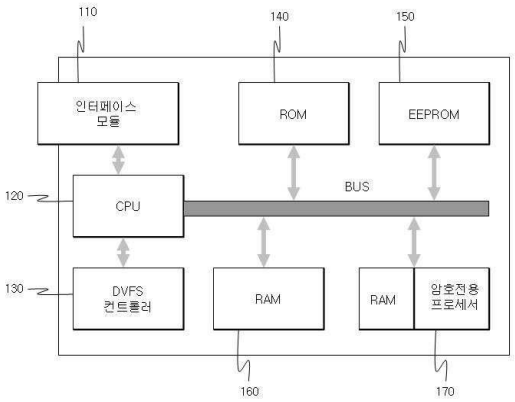
전체 청구항 수 : 총 4 항

(54) 전력 분석 공격 차단을 위한 I C카드

(57) 요 약

본 발명은 전력 분석 공격 차단을 위한 IC카드에 관한 것으로, 더욱 상세하게는 동적 전압 주파수 조절(Dynamic Voltage Frequency Scaling, 이하' DVFS 라고 함) 기술을 이용하여 일반 연산과 보안 연산시 소모되는 전력을 일정하게 유지하여 물리적 해킹 공격인 전력 분석 공격으로부터 안전성을 확보할 수 있는 IC카드에 관한 것이다.

대 표 도 - 도1



특허청구의 범위

청구항 1

CPU와 저장수단을 구비한 IC카드에 있어서,

상기 CPU의 모든 연산 시 소모되는 전력을 일정하게 조절하여 전력 분석 공격을 차단할 수 있는 DVFS 컨트롤러를 포함하는 것을 특징으로 하는 IC 카드.

청구항 2

제 1항에 있어서,

상기 DVFS 컨트롤러는

일반연산과 보안연산시 상기 CPU의 동작 주파수 또는 전압이 미리 설정된 일정 범위내에 속하도록 제어하여 소모되는 전력을 일정하게 유지하는 것을 특징으로 하는 IC카드.

청구항 3

제 1항에 있어서,

상기 DVFS 컨트롤러는

보안연산이 일반연산보다 전력 소모량이 많은 경우 상기 CPU의 주파수 레벨을 낮추거나 전압의 공급을 낮추어 상기 일반연산시 소모되는 전력과 동일 또는 유사하게 조절하는 것을 특징으로 하는 IC카드.

청구항 4

제 1항에 있어서,

상기 DVFS 컨트롤러는

보안연산이 일반연산보다 전력 소모량이 적은 경우 상기 CPU의 주파수 레벨을 높이거나 전압의 공급을 높여서 상기 일반연산시 소모되는 전력과 동일 또는 유사하게 조절하는 것을 특징으로 하는 IC카드.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 전력 분석 공격 차단을 위한 IC카드에 관한 것으로, 더욱 상세하게는 동적 전압 주파수 조절(Dynamic Voltage Frequency Scaling, 이하' DVFS 라고 함) 기술을 이용하여 일반 연산과 보안 연산시 소모되는 전력을 일정하게 유지하여 물리적 해킹 공격인 전력 분석 공격으로부터 안전성을 확보할 수 있는 IC카드에 관한 것이다.

배 경 기 술

[0002] 일반적으로 IC 카드(Intergrated Circuit Card)는 스마트 카드라고 불리는 제 4세대 카드로써, 구조상 내부에 대한 정보의 기록 및 판독이 IC카드 자체가 갖는 연산 처리부의 제어 하에서 행해지기 때문에 자기카드(Magnetic card)에 비해 안전하게 정보를 관리할 수 있다. 따라서 비밀로 저장해야할 정보를 안전하게 관리하기 위한 수단으로 널리 이용되고 있으며, IC카드의 이용분야가 확대되면서 기존의 해킹과는 양상을 달리

하는 물리적 공격(Side Channel Attack) 방법이 등장하면서 IC카드의 물리적 안정성에 대한 관심이 높아지고 있다.

[0003] 여기서, 물리적 공격이란 IC 카드와 같이 암호화, 복호화, 서명 작성 등의 기능을 갖는 장치(Secure Cryptographic Device)에 대한 새로운 위협으로써 IC 카드의 칩 내부에 있는 비밀 키와 같은 중요한 정보를 물리적으로 직접 해석하지 않고, 통상의 사용 방법에서의 처리시간, 소비전류, 발생하는 전자파 등을 물리적 성질을 외부로부터 해석하여 중요한 정보를 추정하는 공격법을 말한다.

[0004] 상기와 같은 물리적 공격에는 TA(Timing Attack), DPA(Differential Power Analysis), SPA(Simple Power Analysis) 등의 공격법이 있으며, 상기 TA 공격은 IC 칩의 암호 알고리즘이 비밀키와 관련된 정보를 처리하는데 걸리는 시간 차를 분석해 비밀 키를 추정하는 타이밍 공격 방법을 말하고, DPA 및 SPA 공격은 비밀 키와 관련된 데이터를 처리할 때 IC 칩이 사용하는 전력량과 그렇지 않을 경우의 전력량을 비교 분석하여 비밀 키와 관련된 정보를 추정하는 전력 분석 공격 방법을 말한다.

[0005] 특히 상기와 같은 물리적 공격 중 DPA 또는 SPA와 같은 전력 분석 공격이 가장 위협적인 공격 방법으로 알려져 있으므로 이와 같은 공격 방법을 방지할 수 있는 대책이 절실히 필요한 실정이다.

[0006]

발명의 내용

해결 하고자하는 과제

[0007] 상기와 같은 문제점을 해결하기 위해 안출된 것으로써, 본 발명의 목적은 DVFS 기술을 이용하여 DPA 또는 SPA와 같은 전력 분석 공격으로 인해 중요한 정보가 노출되는 것을 방지할 수 있는 IC카드를 제공하는 데 있다.

과제 해결수단

[0008] 상기와 같은 목적을 달성하기 위해 본 발명에 따른 IC 카드는 CPU와 저장수단을 구비한 IC카드에 있어서, 상기 CPU의 모든 연산 시 소모되는 전력을 일정하게 조절하여 전력 분석 공격을 차단할 수 있는 DVFS 컨트롤러를 포함하는 것을 특징으로 한다.

[0009] 여기서, 상기 DVFS 컨트롤러는 일반연산과 보안연산시 상기 CPU의 동작 주파수 또는 전압이 미리 설정된 일정 범위내에 속하도록 제어하여 소모되는 전력을 일정하게 유지하는 것을 특징으로 한다.

[0010] 그리고, 상기 DVFS 컨트롤러는 보안연산시와 일반연산시의 전력 소모량을 비교하여 보안연산시의 전력소모량과 일반연산시의 전력소모량이 동일 또는 유사하도록 제어하는 것을 특징으로 한다.

[0011] 보다 구체적으로, 상기 DVFS 컨트롤러는 보안연산이 일반연산보다 전력 소모량이 많은 경우 상기 CPU의 주파수 레벨을 낮추거나 전압의 공급을 낮추어 상기 일반연산시 소모되는 전력과 동일 또는 유사하게 조절하는 것을 특징으로 한다.

[0012] 그리고, 상기 DVFS 컨트롤러는 보안연산이 일반연산보다 전력 소모량이 적은 경우 상기 CPU의 주파수 레벨을 높이거나 전압의 공급을 높여서 상기 일반연산시 소모되는 전력과 동일 또는 유사하게 조절하는 것을 특징으로 한다.

효 과

[0013] 상기에서 살펴본 바와 같이 본 발명에 따른 IC 카드는 DVFS 컨트롤러가 CPU의 모든 연산시 소모되는 전력을 일정하게 유지하여 내부에 저장된 비밀키 또는 중요한 정보를 전력 분석 공격과 같은 물리적 공격으로부터 효과적을 차단할 수 있는 탁월한 효과가 발생한다.

발명의 실시를 위한 구체적인 내용

[0014] 이하, 본 발명의 구체적인 실시예에 대하여 도면을 참조하여 상세하게 설명하기로 한다.

[0015] IC카드는 일반적으로 인식방법에 따라 접촉식, 비접촉식으로 구분될 수 있으며, 마이크로 프로세서 포함 여부에 따라 메모리 카드, 마이크로 프로세서 카드로 구분될 수 있다. 여기서, 본 발명에 따른 IC카드는 상기와 같은 모든 방식의 IC카드에 적용될 수 있다.

[0016] 도 1은 본 발명의 바람직한 실시예에 따른 IC카드의 블럭도이다.

[0017] 도 1을 참조하면, 비밀 키 또는 중요한 정보와 관련된 데이터를 연산(보안 연산)과 일반 데이터와 관련된 연산(일반연산)을 수행하는 CPU(120)와, 접촉 또는 비접촉 방식의 일반 또는 보안 인식 및 데이터 입출력(I/O)을 위한 인터페이스 모듈(110), ROM(140), EEPROM(150), RAM(160) 등의 저장 수단, 비밀 키 또는 암호 관리를 위한 암호전용 프로세서(Crypto Coprocessor)등의 연산수단(170) 및 상기 CPU의 모든 연산 시 소모되는 전력을 일정하게 조절하는 DVFS 컨트롤러(130)를 포함하여 구성될 수 있다. 상기 인터페이스 모듈(110), 저장 수단(140,150,160) 및 CPU(120)는 버스라인을 통해 연결되어 데이터 입출력이 가능하다.

[0018] 여기서, 상기 DVFS 컨트롤러(130)를 제외한 나머지 구성은 IC 카드에 일반적으로 포함되는 구성으로 당업자에게 자명할 뿐만 아니라, 본 발명의 핵심에서 벗어나는 부분이므로 구체적인 설명은 생략하기로 한다.

[0019] 일반적으로 IC 카드의 비밀 키 또는 중요한 정보와 관련된 데이터를 연산할 경우 전력 소비 패턴이 일반적인 데이터를 연산하는 경우와 다르게 변화한다.

[0020] 보다 구체적으로, 마이크로 프로세서(CPU)가 어떠한 연산을 수행하는지에 따라서 전력 소모의 경향이 달라지게 되므로 서로 다른 명령어를 수행할 때마다 전력 소모의 경향도 달라지게 되며, 상기와 같은 마이크로 프로세서의 전력 소모 경향을 파악하게 된다면 비밀 키를 비롯한 중요한 내부 정보를 해커가 용이하게 추정할 수 있다.

[0021] 따라서, 종래의 IC 카드는 마이크로 프로세서의 전력 소모 경향에 대한 파악이 가능하여 물리적 전력 분석 공격에 취약한 문제가 있지만, 본 발명은 상기 DVFS 기술을 이용한 상기 DVFS 컨트롤러를 이용하여 마이크로 프로세서(CPU)가 어떠한 연산 또는 명령어를 수행하더라도 전력 소모를 일정하게 유지하여 전력 분석 공경을 통한 해킹이 불가능해진다.

[0022] 여기서, 상기 DVFS 컨트롤러(130)에서 적용되는 DVFS 기술은 프로세서(CPU)의 전력소모가 주파수에 비례하는 특징을 이용하여 프로세서의 동작 주파수를 줄임으로써 그에 비례하여 구동전압을 감소시키는 기술로서 시스템의 공급 전압과 클럭 주파수를 변경하여 마이크로 프로세서 및 그 주변 회로의 전력소모를 조절하는 기술이다. 이를 이용하여 상기 DVFS 컨트롤러(130)는 일반적인 데이터를 연산하는 경우와 비밀 키 또는 중요한 정보와 관련된 데이터를 연산하는 경우를 비교하여 전력 소모량을 조절하여 전력 소모의 경향을 일정하게 유지되도록 제어할 수 있다.

[0023] 도 2는 본 발명의 제 1 실시예에 따른 DVFS 컨트롤러의 전력 소모량 조절을 방법을 도시한 블럭도이다.

[0024] 도 2를 참조하면 상기 DVFS 컨트롤러(130)가 미리 정해 놓은 범위 안의 주파수로 CPU가 동작하거나 미리 정해 놓은 범위 안의 전압이 CPU에 공급되도록 조절할 수 있다.

[0025] 보다 구체적으로, 상기 DVFS 컨트롤러(130)는 설정된 주파수 범위에 대한 정보 또는 설정된 전압 범위에 대한 정보를 저장할 수 있으며, CPU의 모든 연산 동작이 상기 설정된 범위 내에 분포하는지 여부를 분석하여 동작 주파수 또는 전압을 조절하므로써 전력 소모를 일정하게 유지할 수 있다.

[0026] 여기서, 상기 설정된 주파수 또는 전압의 범위는 프로세서의 설계에 따라 달라질 수 있으며, 모든 명령어에 대한 연산이 가능한 범위 중 전력 소모가 최소가 되도록 결정되는 것이 바람직하다.

[0027] 도 3은 본 발명의 제 2 실시예에 따른 DVFS 컨트롤러의 전력 소모량 조절을 방법을 도시한 블럭도이다.

[0028] 도 3을 참조하면 상기 DVFS 컨트롤러(130)는 보안연산과 일반연산의 전력 소모량을 비교하여 보안연산시 전력 소모량을 일반연산의 전력소모량과 동일 또는 유사하도록 CPU 주파수 또는 전압을 조절할 수 있다.

[0029] 예를 들어, 비밀 키 또는 중요한 정보와 관련된 데이터의 연산(보안연산)이 일반적인 데이터를 연산(일반연산)하는 경우보다 전력 소모량이 크다면 CPU의 주파수 레벨을 낮추거나 전압의 공급을 낮추어 전력 소모량을 일반적인 데이터를 연산하는 경우의 전력 소모량 만큼 낮출 수 있다.

[0030] 그리고, 반대로 비밀 키 또는 중요한 정보와 관련된 데이터의 연산(보안연산)이 일반적인 데이터의 연산(일반연산)보다 전력 소모량이 적다면 CPU의 주파수 레벨을 높이거나 공급되는 전압을 높여서 전력 소모량을 일반적인 데이터의 소모량 만큼 높일 수 있다.

[0031] 따라서, 본 발명은 상기 DVFS 컨트롤러(130)가 비밀 키 또는 중요한 정보와 관련된 데이터의 연산(보안연산)시 소모되는 전력의 경향과 일반적인 데이터와 관련된 연산(일반연산)시 소모되는 전력의 경향을 동일 또는 유사하게 조절하여 전력 분석 공격을 막을 수 있다.

[0032] 이상에서 설명한 본 발명의 상세한 설명에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 본 발명의 보호범위는 상기 실시예에 한정되는 것이 아니며, 해당 기술분야의 통상의 지식을 갖는 자라면 본 발명의 사상 및 기술영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 바람직한 실시예에 따른 IC 카드의 블럭도이다.

[0034] 도 2는 본 발명의 제 1 실시예에 따른 DVFS 컨트롤러의 전력 소모량 조절을 방법을 도시한 블럭도이다.

[0035] 도 3은 본 발명의 제 2 실시예에 따른 DVFS 컨트롤러의 전력 소모량 조절을 방법을 도시한 블럭도이다.

[0036] *도면의 주요부분에 대한 부호의 설명*

[0037] 110 : 인터페이스 모듈 120 : CPU

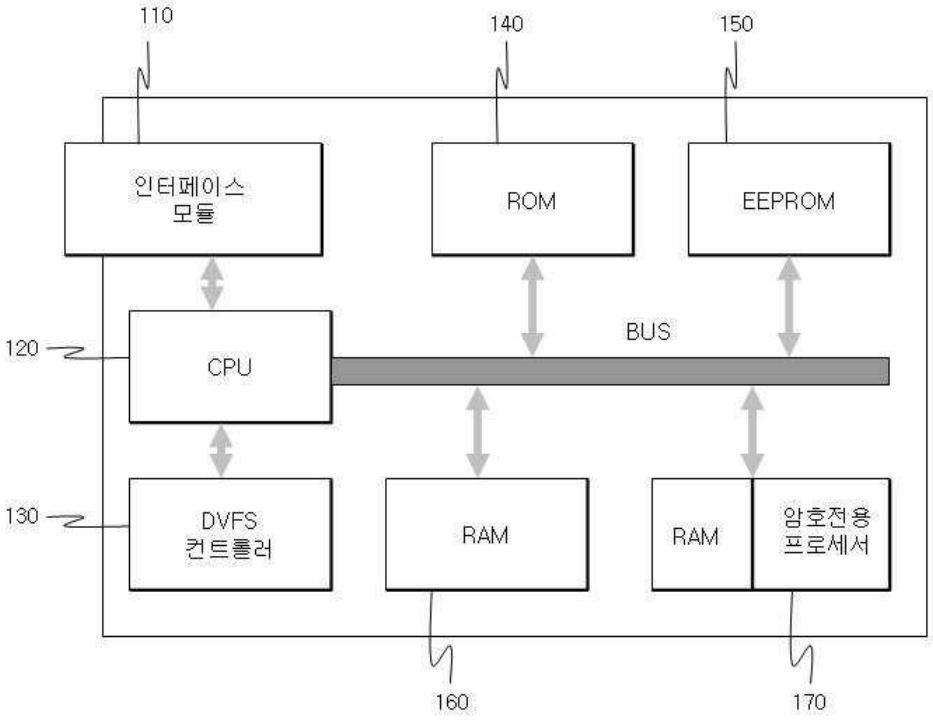
[0038] 130 : DVFS 컨트롤러 140 : ROM

[0039] 150 : EEPROM 160 : RAM

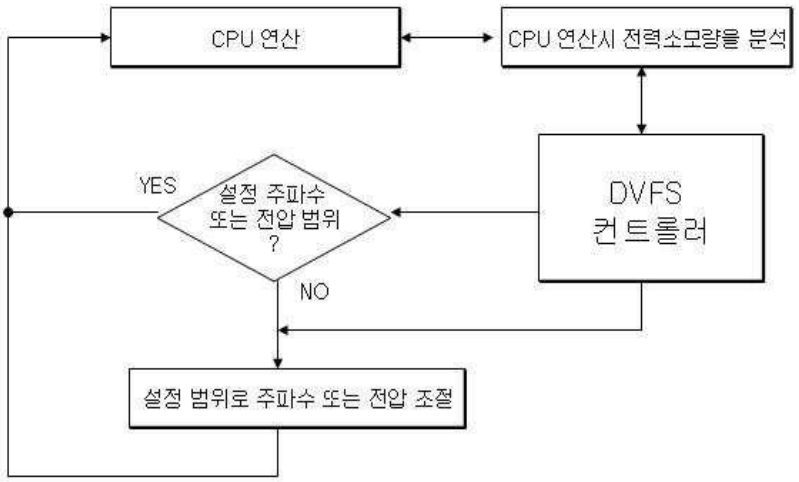
[0040] 170 : 연산수단

도면

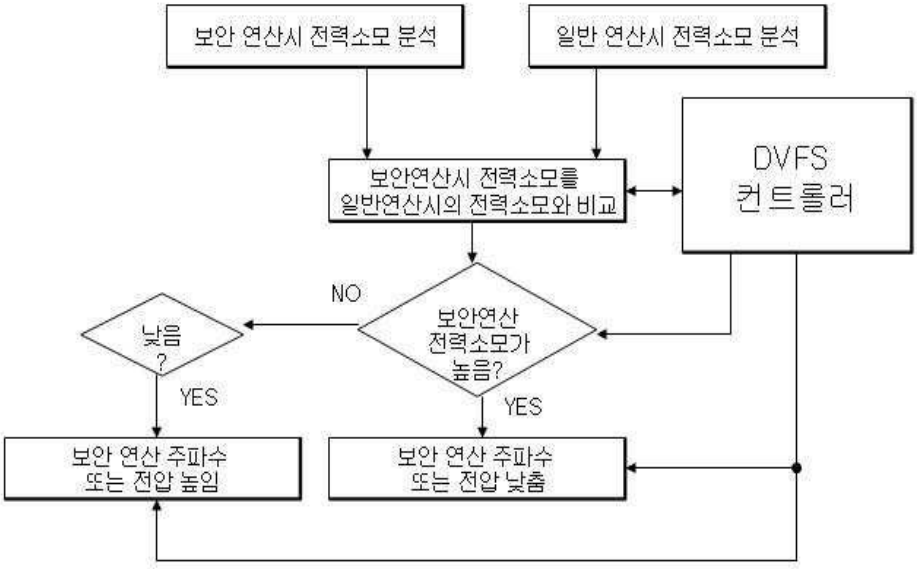
도면1



도면2


CPU 연산
CPU 연산시 전력소모량을 분석
DVFS
컨트롤러
YES
설정 주파수
또는 전압 범위
?
NO
설정 범위로 주파수 또는 전압 조절

도면3


보안 연산시 전력소모 분석
일반 연산시 전력소모 분석
DVFS
컨트롤러
보안연산시 전력소모를
일반연산시의 전력소모와 비교
NO
보안연산
전력소모가
높음?
낮음
?
YES
YES
보안 연산 주파수
또는 전압 높임
보안 연산 주파수
또는 전압 낮춤