보안 칩의 물리적 공격 및 대응 기술 동향

고영운
충남대학교 전자공학과

고형호
충남대학교 전자공학과

Ⅰ. 서 론

IoT(Internet of things) 기반 초연결 사회를 대비하여 세계적으로 보안 칩에 대한 요구가 급증하고 있다. 지금까지 칩을 보호하기 위한 일반적인 보호조치는 소프트웨어 보안기술인 암호화 알고리즘에 의존해왔다. 하지만 칩 내부의 데이터를 얻기 위해서 암호해독, 암호화키와 같은 많은 물리적 공격이 있다[1]. 최근 국내외 여러 기관에서 칩의 물리적 공격에 따른 해킹사고가 일어남에 따라 소프트웨어 보안시스템의 문제점이 크게 제기 되고 있다. 소프트웨어 보안시스템은 시스템의 하드웨어가 물리적 공격에 안전하다는 보장이 있을 때 보안이 확립 될 수 있다. 이렇듯 소프트웨어 보안은 시스템의 물리적 공격에 대한 보안이 확립되어야 안전이 보장된다는 한계가 존재한다. 이러한 소프트웨어 보안 시스템의 한계를 보완하기 위해 다양한 하드웨어 보안시스템이 제안되고 있다. 하지만 하드웨어 보안시스템도 다양한 물리적 공격에 의해 칩 내부의 정보가 노출 될 수 있다[2]. 본고에서는 최근 보안 칩에 대한 물리적 공격 및 이에 대한 대응기술 동향에 대하여 기술한다. 2장 1절에서는 물리적 공격에 대해서 알아보고, 2절에서는 침투공격, 3절에서는 준 침투 공격, 4절에서는 비 침투 공격에 대해서 소개한다. 3장에서는 물리적 공격에 대한 방어기법들을 설명하며, 마지막으로 4장에서 결론 및 연구방향으로 끝을 맺는다.

Ⅱ. 물리적 공격

1. 물리적 공격의 분류

물리적 공격이란 시스템 자체에 물리적인 손상을 가하거나 누설되는 정보들을 고가의 장비 및 기술로 분석하여 공격하는 방법으로 일부 공

〈표 1〉 물리적 공격의 분류

분류 기준	공격 방법	설 명
공격 태도	수동형	암호 모듈을 여러 번 입력하여 원하는 데이터를 획득한다.
	능동형	입출력 및 외부 환경을 이용 및 조작하여 원하는 데이터를 획득한다.
손상 발생 여부	침투형	패키지를 분해하여 내부 구조를 관찰하거나 데이터를 획득한다.
	준 침투형	직접적인 물리적 접근 없이, 레이저 광선 등을 이용한 오류 주입을 수행한다.
	비 침투형	부채널 정보를 이용하여 데이터를 분석 및 획득한다.

격의 경우 매우 효과적인 것으로 알려져 있다. 물리적 공격은 공격태도와 공격 시 손상의 발생 여부에 따라 분류할 수 있다. 공격 태도에 따라서는 수동형 공격과 능동형 공격으로 나눌 수 있고, 손상 발생 여부에 따라 침투 공격 (Invasive attack), 준 침투 공격 (Semi-invasive attack), 비 침투 공격 (Non-invasive attack)으로 나뉜다. 자세한 물리적 공격의 분류는 〈표 1〉과 같다.

2. 침투 공격 (Invasive attack)

침투 공격은 칩 패키지에 직접 접근하여, IC(Integrated circuit)회로를 직접 관측 하거나 칩 내부 구조를 분석하는 공격 방식이다. 고가의 장비와 숙달된 전문 기술이 필요하기 때문에 매우 큰 비용이 필요하나, 각각의 소자나 Metal에 직접 접근하는 것이 가능한 만큼 매우 강력한 공격 수단이다. 이러한 침투 공격은 〈표 2〉와 같이 분류 할 수 있다.

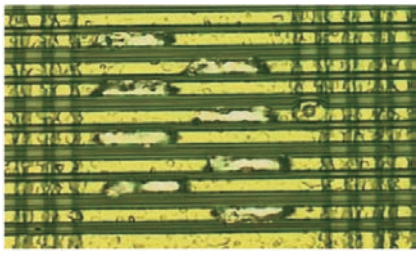
물리적 공격은 공격 태도에 따라 수동형/능동형, 손상 발생 여부에 따라 침투형/준침투형/비침투형으로 분류할 수 있다.

〈표 2〉 침투 공격의 종류

공격 분류	특 징
De-packaging	회로에 접근하기 위해 회로를 덮고 있는 물질을 제거한다.
Layout reconstruction	관찰을 통해 프로세서의 전체적 구조를 습득하고 재설계를 통해 모든 메모리에 접근한다.
Probing	Probe를 이용하여 정보를 읽거나 변경, 주입한다.
메모리 읽기/쓰기/변경	메모리 소자(ROM, RAM, EPROM, EEPROM 등)의 내용을 읽거나 변경한다.
회로 수정	FIB를 이용하여 fuse를 연결해 test-mode를 재동작시키거나 일부 회로를 파괴해 오동작 유발시킨다.

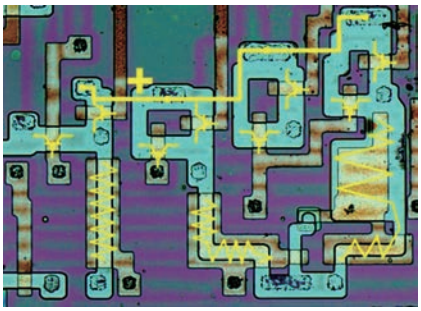
〈표 3〉 De-packaging 공격의 종류

구 분	설 명
Manual material removal	칼과 다른 도구를 사용하여 센서가 짧은 시간 중지되었을 때 커버를 제거한다.
Mechanical machining	기계를 이용한 방법으로 많은 양의 물질을 매우 정확하고 빠르게 제거된다. 그러나 피드백이 없어 너무 깊게 자르는 경우도 발생한다. 또한 칼이 전도성이기 때문에 침입 탐지기에 의해 탐지될 수 도 있다.
Chemical machining	대부분의 물질은 녹일 수 있기 때문에 높은 압력의 스프레이 형태로 용액이나 산을 사용하여 코팅을 제거한다. 다만 높은 전도성으로 인해 합선이 발생할 수 있다.
Water machining	물을 이용한 방법으로 매우 정확한 방법이다. 순수한 물을 사용할 경우 비전도체이기 때문에 특히 부드러운 물질에 효과적이다. 그러나 비용과 크기(기기의 크기가 큼)가 상당히 큰 단점이 있다.
Laser machining	Water machining과 비슷한 장점들은 가지나 많은 열을 발생시키는 단점이 있다. 그리고 제거하려는 물질에 맞게 레이저를 조정해야 한다.
Shaped charge technology	매우 정확하며 빨라 회로가 응답하기도 전에 구멍을 뚫는 것이 가능하다.



〈그림 1〉 De-packaging 공격에 관찰된 칩 내부[3]

De-packaging 공격은 칩 내부를 관찰하기 위해 외부 물질을 제거하는 과정으로 사용하는 도구 및 방법에 따라 〈표 3〉과 같이 나뉜다. Water machining, Laser machining, Shaped charge technology 등은 특수한 장비가 필요하나 그만큼 정밀한 공격이 가능하다. 이러한 방법들은 높은 비용이 필요하나 나머지 기술들의 조합으로도 간단히 De-packaging이 가능하다. 우선 칼을 이용하여 플라스틱을 제거하고 뒷부분의 Epoxy resin 부분이 보일 때 까지 벗겨낸다. 그리고 Resin을 녹이기 위해 질산염을 몇 방울 떨어뜨린 뒤, 실리콘 층이 전부 보일 때까지 아세톤에 넣고 흔들어준다. 산에 Resin이 전부 씻겨 나가면, 칩에 대한 본격적인 물리적 공격이 가능하다. 이러한 De-packaging을 통해 관

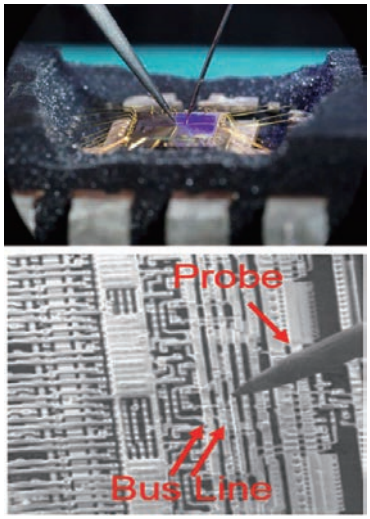


〈그림 2〉 Reverse engineering을 통한 회로 회로 reconstruction[3]

찰된 칩의 내부는 〈그림 1〉과 같다[3].

Layout reconstruction 공격은 칩의 Layout을 얻어내는 공격으로, 공격자는 Metal 층들을 벗겨내면서 CCD(Charge coupled device) 카메라가 장착된 광학 현미경을 통해 칩 표면의 각 층별로 고해상도 이미지를 획득한다. 프로그램을 통해 이미지 해상도를 조절해가며 Metal 층들을 관찰하는 것이 가능하며, 특히 ROM, RAM, EEPROM 등의 IP나 이들에 연결된 Address bus line / Data 등은 쉽게 분간이 가능하다. 획득한 이미지를 바탕으로 재구성(Reverse engineering)된 Layout 정보는 추후 Probing 공격이나 칩의 회로를 수정할 때 유용하게 사용된다. CCD 카메라 대신 X-ray, Tomography, Ultrasound 등을 사용하여 패키지 내부의 모습을 영상화하는 방법도 존재한다. Layout reconstruction 공격을 통해 재구성된 회로의 예시는 〈그림 2〉와 같다[3].

Probing 공격은 Probe를 이용하여 Metal 층의 데이터를 읽거나 변경, 또는 주입하는 공격이다. 이와 같이 〈그림 3〉은 Probe를 통해 칩 내부의 Bus line을 공격하는 것을 나타낸다. 가장 많이 사용되는 방법은 Energy probe로 Ion beam과 Electron beam이 있다. Ion beam은 Vacuum chamber와 Particle gun을 탑재한 장비이며, 갈륨이온 빔을 사용하여 전류의 강도를 조절하여 값을 관찰하고 회로를 수정할 수 있다. Ion beam장비를 사용하여 갈륨이온의 빔 투사로 튀어나온 이온(i+), 중성자(n0), 전자(e−)를 분석하여 Metal 층을 관찰할 수 있고, 빔의 강도를 높이거나 빔에 가스를 첨가하여 Metal 층을 절단하거나 연결할 수 있다. Ion beam 장비의 원리는 〈그림 4〉와 같다.

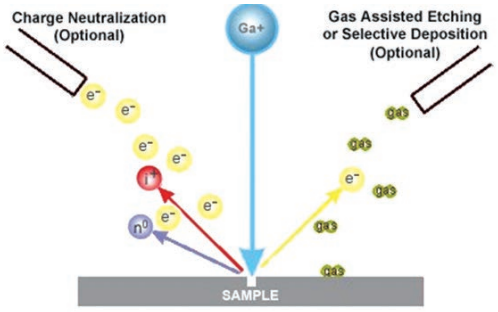


〈그림 3〉 Probe를 통해 회로를 공격하는 과정[4]

〈표 4〉 Probing 공격의 종류

구 분	설 명
Passive probe	Oscilloscope나 logic analyzer probe를 이용하여 정보를 읽어낸다.
Active or Injector probe	Pattern generator와 비슷한 장비를 상용하여 신호나 정보를 주입한다.
Pico-probe	정보를 읽거나 주입 가능하며 매우 작아 직접 IC 표면 Probe 가능하다.
Energy probe	Electron beam, Ion beam, Focused beam 등으로, 반도체 저장소의 내용을 읽거나 쓸 수 있으며, 제어 신호를 변경할 수 있음. Ion beam의 경우 Fuse를 다시 이어 디버그 상태가 가능한 생산 단계로 변경하는 것이 가능하다.

Electron beam장비는 빛 대신 전자를 사용하여 마이크론 단위보다 더 작은 칩도 분석이 가능하다. Condenser lens를 통해 에너지를 집중하고 Deflection coil을 가지고 방향을 수정할 수 있다. 아래쪽의 샘플에 빔 충돌 시 튀어나온 X-ray와 전자를 감지하고, 전력 값(0, 1)에 따라 색이 달라져 버스 값을 실시간으로 관찰하



〈그림 4〉 Focused ion beam의 원리

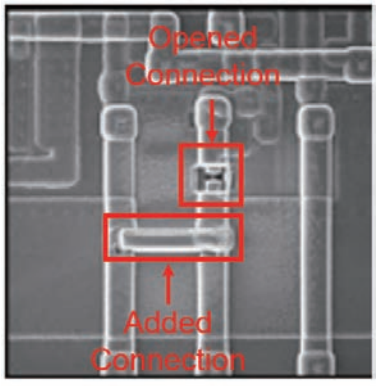
〈표 5〉 메모리 공격방법

구 분		설 명
ROM	Reading	ROM에 저장된 Access control, Cryptographic routines 등의 정보를 읽어 다른 공격에 이용한다.
	Over writing	레이저 등의 장비를 이용하여 특정 bit을 수정하여 암호화 과정 등을 수정한다.
RAM	Imprinting/ remanence	X-ray, 높은 전압, 낮은 온도 등의 환경 요인을 조절하여 RAM의 내용이 삭제(전원 제거 또는 Rewrite) 되는 것을 방지한 후 값 읽어낸다.
EEPROM	Over writing	값을 읽어내는 것은 어려우나 특정 bit의 값을 쓰는 것이 가능할 경우 내부의 오류 정정(Parity error)를 이용하여 1-bit씩 추측 가능하다.
	Lock 해제	UV light를 이용하여 읽기 금지되어 있던 Security lock을 지워 메모리 값을 읽어낸다.
일반 메모리	Bus probing	메모리에/로부터 쓰이거나 읽히는 데이터는 반드시 Bus를 통하기 때문에 Bus를 Probing하여 데이터 획득한다.

여 칩 구조를 이미지화 할 수 있다.

메모리 공격은 공격 대상에 따라 읽기, 쓰기, 변경하는 방법이 있고, 공격 대상 메모리로는 ROM, RAM, EEPROM 등이 있으며, 이들에 대한 공격 방법은 〈표 5〉와 같다.

회로 수정 공격은 FIB(Focused ion beam) 등의 장비를 이용하여 Fuse를 재연결하거나 일부 회로를 파괴시키는 공격방법이다. 〈그림 5〉는 FIB를 이용한 회로 수정 공격을 나타낸 그림이다[4].



〈그림 5〉 FIB를 통해 회로를 공격하는 과정[4]

Fuse는 특정 값을 영구적으로 고정시키기 위한 용도로 사용되며, 그 예로 제품 시판 전 칩 테스트를 위해서만 Test-mode를 사용하기 위해 테스트 후 Fuse를 단절시켜 Test-mode로의 진입을 방지하는 방법이 있다. 보통 Test-mode는 테스트를 위해 모든 권한을 가지고 있어 모든 내부 회로에 접근 및 제어할 수 있는 것이 일반적이다. 따라서 Test-mode가 재활성화 된다면 비밀 정보를 손쉽게 읽어내는 것이 가능하다.

이러한 공격 외에도 보안과 관련된 연산을 수행하는 회로를 파괴할 경우 암호화 등의 연산이 제대로 되지 않아 쉽게 키 값이나 암호화를 통해 보호했어야 하는 비밀 정보들이 그대로 노출될 수 있다.

3. 준 침투 공격 (Semi-Invasive attack)

칩에 직접적인 물리적 접근 없이, 레이저 광선 등을 이용하여 오류를 주입하고 그에 따른 오동작을 분석하는 공격 방식이다. 칩의 Packaging을 제거한 후 오류를 유발시키는 방법과 외부에서 전기적 스파이크를 일으켜 오류를 유발시키는 방법 등이 있다. 공격 방법에 따라 De-package가 필요한 경우도 존재하며, 이 경우 칩은 동작 가능한 상태로 패키지를 제거할 수 있어야 한다. 준 침투 공격을 통해 오류를 유발하는 방법은 〈표 6〉과 같다. 오류는 원상복구의 유무에 따라 Provisional / Transient fault, Destructive / Permanent fault로 크게 두 가지로 분류할 수 있다. Provisional / Transient fault는 일시적이라 원상복구가 가능하여 오류 요인 중단 시 칩은 일반 상태로 복구할 수 있다. 따라서 공격 후 시스템 동작이 가능하므로 동일 칩에 많은 실험이 가능하다. Destructive / Permanent fault는 영구적으로 원상복구가 불가능하여 칩의 전체 구조를 수정하는 방식의 공격이다. 위의 두 가지 오류의 종류는 〈표 7〉과 같다[5].

침투 공격은 De-packaging, probing, FIB 를 이용한 회로 수정 등을 이용하여 칩 내부를 직접 관측하고 회로 구조를 분석하는 강력한 공격 수단이다.

4. 비 침투 공격 (Non-invasive attack)

비 침투 공격은 부채널 공격(Side channel Attack)을

〈표 6〉 준 침투 공격의 오류 유발 방법[5]

구 분	설 명
전압 변화	전압을 비정상적으로 바꾸는 방법으로 정확한 타이밍이 필요하지 않다. 균일하게 오류가 발생하여 크기에 상관없이 효과적이며, 쉽고 증거가 남지 않는다.
Power supply glitch	전압 공급 시 Spike나 Brownout을 발생시켜 특정 주기에서 명령어가 수행되지 않도록 한다. 별도로 제작한 회로로 동기와 지속시간을 정확히 맞출 수 있어야 한다. (상호 유도 현상으로 인해 어려움)
Clock 변화	클락 주기를 늘리거나 줄여서 오동작을 유발한다. 공격 장비는 공격 대상보다 빠른 Clock 스피드를 가지고 있어야한다. (제품들의 속도가 계속 빨라지고 있어 공격도 어려워지고 있음)
Clock glitch	Glitch를 주입하여 오동작을 유발한다.
Xray & Ion beams	X-ray, Ion beams 등으로 RNG나 일부 회로의 오동작을 유발한다. De-packaging 없이 공격 가능하다. (방어 대책이 적용된 특수 Package된 경우 De-packaging 필요)
Heat	온도가 올라갈 경우, DRAM에서 오류가 발생한다. (100℃ 이상에서 32-bit 워드 당 약 10-bit이 반전됨) 너무 강한 열에 의해 회로가 파괴될 수 있음
High energy light	매우 짧은 순간 집중된 빛을 비추고, 광전효과로 인한 전류를 통해 오류를 유발한다. UV lamp를 통해 Erasable EPROM이나 FLASH 메모리 셀의 내용을 지울 수 있다.
Laser	방향성으로 인해 매우 좁은 특정 부분 집중 가능하다. 강도, 파장, 지속력, Spot size 등을 조절하기 쉽다. 필요비용이 White light보다 고가이다.

〈표 7〉 준 침투 공격의 오류 종류[5]

구 분	종 류
Provisional / Transient fault	Single event upsets (SEUs) : 일시적인 Bit flip 유발하여, Clock이나 공급전압의 조작이 가능하다. Multiple event upsets (MEUs) : SEU가 동시에 복수로 발생하여 문제 발생 확률이 높아, 오류주입공격의 주된 공격 방식이다.
Destructive / Permanent fault	Single event latchup (SELs) : Power와 Ground를 합선시켜 이로 인한 높은 전류로 칩 손상을 일으킨다. Single event burnout faults (SEBs) : power transistor를 파괴하여 유발된 높은 온도로 칩을 손상시킨다. Single event gate rupture (SEGRs) : Leakage current 증가가 원인이 되어 Gate oxide가 붕괴된다. Single event snap back faults (SESs) : SELs와 비슷하며, NMOS 트랜지스터에서만 발생한다.

통해 데이터를 분석 및 획득하는 공격이다. 이러한 부채널 공격은 칩이 동작할 때 물리적 공격을 통해 누설되는 비밀 정보를 이용할 수 있다. 이 공격은 대부분 중요한 암호화 알고리즘을 파괴할 수 있는 강력한 공격이다[1]. 부채널 공격은 부채널 정보에 따라 시차 공격, 전력 분석 공격, 전자기파 분석 공격 등으로 분류할 수 있다.

시차 공격은 각각의 입력 데이터에 따라 달라지는 연산의 시간이나 연산 회수를 관찰하여 분석하는 방법이다[2, 6]. 전력 분석 공격은 공격 대상의 전력 소모를 통해 비밀 키를 추출하는 방식으로 부채널 공격 중 가장 위협적인 공격이다 전자기파 분석은 공격 대상 암호 장치로부터 방사되는 전자기파 신호를 분석하는 방법이다.

원거리에서 정보의 습득이 가능하며 다중 채널로 구성되고 있어서 전력 분석 공격 대응 장치에서도 전자기파 정보의 분석이 가능하다는 장점이 있다[2, 7]. 자세한 부채널 공격의 종류는 〈표 8〉과 같다.

Ⅲ. 물리적 공격에 대한 방어 기법

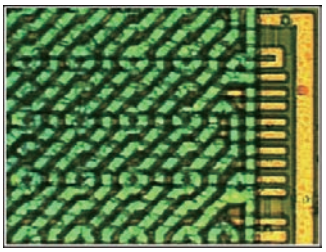
1. 침투 공격의 방어기법

앞서 살펴본 침투 공격은 크게 De-packaging, Layout reconstruction, Probing, 메모리 읽기/쓰기/변경, 회로 수정이 있었다. 침투 공격과 오류 주입 공격은 De-packaging이 우선적으로 수행되어야 한다. 따라서 De-packaging을 방지하거나 De-packaging된 사실을 회로에서 감지할 수 있다면 공격을 대처할 수 있다. 이 외에도 De-packaging 되더라도 내부 구조를 분석하기 어렵게 하거나 비밀 정보의 경우 암호화하는 방법이 사용될 수 있다.

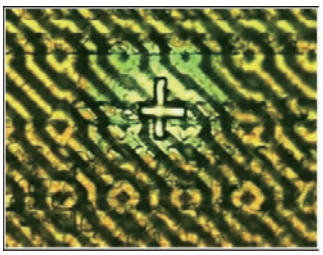
먼저 De-packaging을 감지하기 위한 방법으로

〈표 8〉 부채널 공격의 종류

구 분	종 류
시차공격 [2, 6]	대표적인 공개키 알고리즘인 RSA의 경우 키의 각 bit 값에 따라 내부에서 수행되는 연산의 종류가 달라지므로 이를 관찰하여 키 값을 추출한다.
전력 분석 공격 [2, 7]	단순 전력 분석(Simple power analysis : SPA) : 특정명령어가 수행되는 한 시점에서 데이터에 따라 달라지는 소비전력을 분석하여 비밀정보를 유추하는 방법이다. SPA는 공격자가 공격하고자 하는 시점의 구현 방법을 정확히 알고 있어야 하는 단점이 있다. 차동 전력 분석 (Differential power analysis : DPA) : 비밀정보 bit와 소비전력의 통계적인 상관관계를 이용하여 비밀 정보를 유추할 수 있는 방법으로 노이즈에 강인하고 아주 적은 자원을 사용하기 때문에 가장 강력한 공격방법이다.
전자기파 분석 공격[7]	단순 전자기파 분석 (Simple electro-magnetics analysis : SEMA)과 차동 전자기파 분석 (Differential electro magnetics analysis : DEMA) 은 SPA와 DPA 기술을 전자기파로 측정하는 공격으로 소비전력이 측정되지 않을 때 유용한 방법이다.



〈그림 6〉 Top layer Sensor mesh의 모습[3]



〈그림 7〉 FIB chip editing을 이용한 Sensor mesh 공격[3]

Sensor mesh 기법이 있다. Top metal layer에 Sensor mesh layer를 삽입하여 Metal이 일부 훼손될 경우 이를 감지하여 내부 동작을 중지하는 등의 방어 기법을 수행하는 방법이다. Top layer sensor mesh방어 기법은 〈그림 6〉과 같다. 그러나 Metal의 구조가 파악될 경우 FIB 등을 이용하여 구멍을 뚫거나 우회하는 것이 가능하다. 〈그림 7〉은 FIB에 의해 뚫린 Sensor mesh의 모습이다[3].

각종 공격을 방어하기 위해 top layer sensor mesh, 공격 감지 센서, 오류 검출 코드 (EDC), 누설 전류 감소 등 다양한 방어 기법이 연구되고 있다.

Layout 분석을 어렵게 하기 위한 방법으로는 Dummy 모듈 방법이 있다. Dummy 모듈이나 Dummy bus를 추가하여 칩의 분석을 어렵게 하고, 그 외에도 시차의 연산 시간, 전력 소모 등의 변화를 통해 Leakage reduction에도 유용하다[1]. 그러나 Dummy 만큼 면적과 비용이 증가하는 단점이 있다.

메모리 공격에 대한 방어기법으로는 암호화, Data / Address scrambling 방법이 있다. 메모리에 내용물을 암호화하여 저장하거나 Data Bus나 Address Bus를 Scramble하는 방법으로 저장된 값을 검색해내기 더 어려워지나 칩 성능이 저하된다는 단점이 있다. 블록 암호를 이용한 암호화 기법으로는 관련 표준으로 IEEE P1619TM/D16(Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices)이 존재한다.

2. 준 침투 공격의 방어 기법

오류를 발생시키기 위하여 비정상적인 환경(너무 높거나 낮은 전압 또는 온도 등)이 조성되거나 빛이나 레이저 등이 사용되므로 이를 감지할 수 있는 센서를 갖추거나 외부의 영향을 받지 않도록 내부에서 전압이나 Clock 주파수를 통제하도록 하는 방법이 사용된다.

센서 방어 기법은 온도, 자외선, 적외선, X선, 전리 방사선, Clock 주파수, 전압 등을 감지하는 센서를 내장한다. 특정 범위를 벗어날 경우 동작을 중지하는 등의 방어 기법을 수행한다. 그러나 센서들도 전압이 필요하므로 전압을 차단함으로써 무력화시킬 수 있는 단점이 있다.

전압 및 Clock 제어 모듈을 내장하는 방어기법은 칩 내부에 안정적으로 전압을 제공할 수 있는 모듈이나 자체적으로 Clock을 발생시킬 수 있는 PLL 모듈을 내장함으로써 외부의 전압이나 Clock 주파수 변화 또는 Glitch 유발에도 영향을 받지 않도록 한다[3].

Error detecting code (EDC) 사용하는 방어기법은 EDC를 사용하여 매 주기마다 또는 맨 마지막에 오류가 발생했었는지 확인한다. 설계 변경 기법에 비해 Overhead가 적으나 방법에 따라 오류를 100% 잡아내지 못할 수 있다. 알고리즘에 따라 EDC는 달라지며, 최근 RSA의 지수 연산과 ECC의 곱 연산에 대하여 SPA/DPA 공격과 Fault Injection 공격을 방지할 수 있는 Unified countermeasure 기법 연구되기도 하였다[7].

Packaging 방어 기법은 EM 공격의 경우 De-packaging 없이는 공격이 가능하나 Grounded metal packaging을 통해 EM fault 공격을 방지할 수 있다. 그러나 이 경우에도 De-packaging을 통해 Shield를 무력화시킬 수 있는 단점이 있다.

3. 비 침투 공격의 방어 기법

부채널 공격의 방어 기법의 종류로는 Leakage

reduction, Noise injection, Key update, Secure scan chain 등이 존재한다.

Leakage reduction 방어 기법은 부채널에 흐르는 전류와 비밀정보 사이의 의존성을 감소 시켜야한다. 예를 들어 시차 공격에 대해서 RSA의 지수연산을 고려하면 공개키 알고리즘에 Dummy를 추가하여 연산을 수행해서 시간 정보와 비밀 지수가 감소하게 되는 효과를 얻는다. 그러나 이외에도 부채널 공격에는 전력소모, 전자기파 분석 등이 있기 때문에 완전히 방어할 수 없다. 따라서 전력분석 공격을 막기 위해서는 Dynamic, Differential logic, Asynchronous logic, Current-mode logic, DRP(Dual-rail precharge logic style) 회로 방식을 사용하면 부채널의 SNR(Signal to noise ratio)이 감소하여 효과적으로 방어할 수 있다.

Noise injection 방어 기법은 SNR을 측정하여 부채널에 인공적인 Noise를 주입하여 부채널 정보를 감소시키는 방법이다. 공격자는 주입되는 Noise로부터 암호화 키와 관련된 정보를 얻기 어려워진다.

Key update 방어 기법은 비밀 키를 자주 최신화 시켜주어 부채널에 정보가 축적되는 것을 막는 방법이다. Key update 기법은 Derivation, Key tree 등 몇 가지 방법이 있다.

Secure scan chains 방어기법은 회로의 민감한 부분에 Mirror key registers를 사용한다. 이러한 레지스터 블록은 테스트 모드에서 민감한 레지스터 값에 무단으로 접근하는 것을 차단해준다. 또 다른 방법으로는 Scan chains을 Sub chains으로 구분하고 일반 사용자들이 무작위로 접근할 수 있도록 한다[1].

Ⅵ. 향후 연구 및 결론

본 고에서는 보안 칩의 물리적 공격 및 이에 대한 대응 기술 동향에 대하여 살펴보았다. 위에서 살펴본 물리적 공격 기법과, 이에 대한 방어 기법은 지속적으로 발전하고 있다. 전 세계적으로 보안 칩의 물리적 공격 및 방어 기법에 대한 관심이 높아지고 있으며, 미국 DAPRPA에서도 VAPR(Vanishing programmable resource) 등의 사업을 통하여 소멸 명령에 따라 산산조각 나는 반도체, 화학적으로 녹아내리는 반도체, 배터리, 체내에서 녹아 없어지는 센서 등이 개발 되고 있다. 향후 보안 칩의 물리적 공격에 대한 대응 기술의 중요성은 점차 증대될 것으로 보이며, 관련 분야의 중점적 연구 및 지원이 필수적이다.

참고문헌

[1] Rostami, Mohamad, Farinaz Koushanfar, and Ramesh Karri. "A primer on hardware security: Models, methods, and metrics." Proceedings of the IEEE 102.8 (2014): 1283-1295.

[2] 최필주, 최원섭, 김동규, "하드웨어 칩 기반 보안시스템 및 해킹동향", 한국통신학회지, 2014. 4, 46-52 (7 pages)

[3] Oliver Kommerling, Markus Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", USENIX Workshop on Smartcard Technology Proceedings, Chicago, Illinois, USA, May 10-11, 1999.

[4] Briais, S., Cioranesco, J. M., Danger, J. L., Guilley, S., Naccache, D., & Porteboeuf, T. (2012, September). Random active shield. IEEE Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 (pp. 103-113)

[5] Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., & Whelan, C. (2006). The sorcerer's apprentice guide to fault attacks. Proceedings of the IEEE, 94(2), 370-382.

[6] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." Advances in Cryptology-CRYPTO'96. Springer Berlin Heidelberg, 1996.

[7] Kocher, P., Jaffe, J., Jun, B., & Rohatgi, P. (2011). Introduction to differential power analysis. Journal of Cryptographic Engineering, 1(1), 5-27.

고영운

• 2015년 8월 충남대학교 전자공학과 학사
• 2016년 3월 ~ 현재 충남대학교 전자공학 석사과정

〈관심분야〉
아날로그 집적회로, 센서 인터페이스, 회로 보안 기술

고형호

• 2003년 2월 서울대학교 전기공학부 공학사
• 2008년 8월 서울대학교 전기공학부 공학박사
• 2008년 11월~2010년 8월 삼성전자 반도체 사업부 책임연구원
• 2010년 9월~현재 충남대학교 전자공학과 조교수/부교수

〈관심분야〉
아날로그 집적회로, 회로 보안 기술, 센서 인터페이스, 생체신호 계측회로, 데이터 컨버터