스캔 기반 사이드 채널 공격에 대한 새로운 AES 코아 키 보호 기술

(A New Key Protection Technique of AES Core against Scan-based Side Channel Attack)

송 재 훈 † 정 태 진 †† 박 성 주 †††
(Jaehoon Song) (Taejin Jung) (Sungju Park)

요 약 본 논문은 Advanced Encryption Standard(AES) 암호화 코아가 내장된 System-on-a-Chip(SoC)의 스캔 기반 사이드 채널 공격에 의해 발생될 수 있는 비밀 키 정보 누출 방지를 위한 효과적인 시큐어 스캔 기술을 제안한다. 본 논문에서 제안하는 시큐어 스캔 설계 기술은 어플리케이션에 최적화 되어있는 암호화 IP 코아를 수정하지 않고 적용을 할 수 있다. 또한 SoC 상의 IEEE1149.1 제어기 표준을 유지하며 기존 방식보다 적은 면적 오버헤드와 전력 소모 및 높은 고장 검출율을 갖는 기술을 제안한다.

키워드 : AES, 키 누출 방지, 스캔 디자인, SoC

Abstract This paper presents a new secure scan design technique to protect secret key from scan-based side channel attack for an Advanced Encryption Standard(AES) core embedded on an System-on-a-Chip(SoC). Our proposed secure scan design technique can be applied to crypto IP core which is optimized for applications without the IP core modification. The IEEE1149.1 standard is kept, and low area and power consumption overheads and high fault coverage can be achieved compared to the existing methods.

Key words : AES, key protection, scan design, SoC.

1. 서 론

Advanced Encryption Standard(AES) 암호화 알고리즘은 스마트 카드와 Zigbee, Bluetooth와 같은 통신용 칩이나 방송용 수신 칩등 보안이 필요한 많은 분야에서 활발히 사용되고 있으며, IP 코아 설계물로 구현되어 정보의 암호화를 필요로 하는 System-on-a-Chip (SoC) 내부에서 많이 사용 되고 있다[1]. 이러한 AES와 같은 암호화 코아에서 사용하는 사용자 비밀 키 정보가 누출 된다면 매우 큰 경제적 손실 및 사회적 문제로 야기될 수 있다. 그렇기 때문에 AES 암호화 코아에 사용되는 사용자 비밀 키 누출을 방지하는 것은 매우 중요한 문제이다.

SoC의 양산 테스트 시 테스트 비용을 절감하고 고장 검출율을 효과적으로 높이기 위해 스캔 설계 기반 테스트가 널리 사용되고 있다[2]. 일반적으로 칩은 출하 전에 스캔 테스트를 통하여 불량품을 선별하는 과정을 거친다. 하지만 테스트를 거쳐 출하되어 소비자가 사용하고 있는 AES IP 코아가 내장된 SoC에 스캔 테스트를 다시 진행하면 사용자 비밀 키와 관련된 정보가 누출될 수 있으며 이렇게 누출된 정보를 이용하여 사용자 비밀 키를 유추해 낼 수 있는 문제가 존재하게 된다[3,4]. 그렇기 때문에 출하 후 AES 코아의 사용자 비밀 키가 스캔테스트 방법에 의해 유출되는 것을 방지하면서 출하전의 테스트 단계에서는 테스트의 질을 높일 수 있는 메커니즘이 필요하다[5].

· 본 연구는 반도체설계교육센터(IDEC)의 지원을 받아 수행되었으며 지식경제부가 지원하는 국가 반도체 연구개발사업인 "시스템집적반도체기반기술개발사업(시스템 IC 2010)"을 통해 개발된 결과임을 밝힙니다.

† 정 회 원 : 한양대학교 컴퓨터공학과
jhsong@mslab.hanyang.ac.kr
†† 학생회원 : 한양대학교 컴퓨터공학과
tjjung@mslab.hanyang.ac.kr
††† 종신회원 : 한양대학교 컴퓨터공학과 교수
parksj@mslab.hanyang.ac.kr

논문접수 : 2008년 4월 18일
심사완료 : 2008년 12월 12일

정보과학회논문지: 시스템 및 이론 제36권 제1호(2009.2)

본 논문에서는 이미 소비자에 의해 사용되어지고 있는 AES 코아가 내장된 칩의 스캔 테스트 시 사용자 비밀 키 누출 방지를 위한 효과적인 설계기술을 제안한다. 기존방법[6,7]과 비교하여 매우 적은 면적 및 전력소모 오버헤드를 갖으며 IEEE 1149.1 표준(이하 JTAG이라 함) 테스트 제어기와의 호환성을 유지하고 AES IP 코아의 재사용성이 높은 기술을 제안한다. 2장에서는 AES 코아의 키 노출 방지를 할 수 있는 기존 스캔 테스트 방법을 소개한다. 3장에서는 본 논문에서 제안하는 기술을 소개하며 4장에서 실험 결과를 보여준다. 마지막으로 5장에서 결론을 맺는다.

2. AES 키 정보 누출 방지를 위한 스캔 테스트 설계 기술

AES[1]의 장점은 하드웨어나 소프트웨어적으로 구현했을 때 모두 좋은 성능을 보이며 구현이 쉽고 메모리를 적게 소모한다는 것이다. AES는 128비트의 데이타와 128, 192 또는 256비트의 사용자 키로 암호화가 이뤄지며 키 길이에 따라 라운드 횟수는 10, 12, 14로 정해진다. 암호화 과정 중 키와 관련된 데이타는 AES 내부의 레지스터에 저장된다. 그림 1과 같이 AES는 한번의 프리 라운드를 거친 후 사용자의 키의 길이에 따라 정해진 라운드 횟수만큼 암호화가 진행된다. 프리 라운드에서는 사용자 비밀 키와 암호화 하고자 하는 평문을 사용하여 KeyXOR 절차를 거친 뒤 데이타 a를 출력하고, 각 라운드에서는 사용자 비밀 키가 확장된 라운드 키와 데이타 a를 이용하여 데이타 e를 출력한다. 데이타 e는 각 라운드의 데이타를 저장하기 위한 레지스터인 Register R에 저장 되어 지는데 이러한 레지스터들은 스캔 테스트를 위한 스캔 체인에 속하게 된다. 스캔 테스트 방법으로 암호화 과정 중 사용자 비밀키가 적용된 데이타 정보가 스캔 출력포트를 통하여 유출이 된다면 공격자는 이렇게 얻은 데이타를 이용하여 사용자 비밀 키를 유추해 낼 수 있다[3-5]. 스캔 테스트 방법으로 발생할 수 있는 AES 사용자 비밀 키 누출 방지를 위해 [6]에서는 스캔 출력포트를 활성화 시킬 수 있는 길이가 N인 서로 다른 M개의 매칭 키를 정의하여 해당하는 모든 매칭 키가 [7]에서 제시한 패턴 매칭 블록 회로에 정해진 순서대로 인가됐을 경우 스캔 출력포트를 활성화 시킴으로써 AES 키 정보 누출을 방지하는 기술을 제안하였다. 하지만 이 기술은 스캔 출력포트 활성화를 위한 M개의 매칭 키를 키 매칭 블록으로 인가하기 위해 AES 내부의 스캔 플립플롭의 출력 팬아웃을 증가시킴으로써 AES 설계에 추가적인 딜레이 및 라우팅 오버헤드를 증가 시킨다. 또한 테스트 엔지니어는 스캔 출력포트를 활성화 시킬 수 있는 매칭 키 값을 알고 있기 때문에 테스트엔지니어에 의해 패턴 매칭 키 값이 누출이 된다면 공격자는 이를 이용하여 AES의 내부 정보를 볼 수 있다. 그렇기 때문에 테스트 엔지니어의 양심적인 의무가 필요하게 된다. [6]에서 제시한 방법은 이미 구현되어 있는 AES IP코아의 수정이 필요하기 때문에 AES 코아의 재사용이 어렵다는 단점을 갖으며 스캔테스트를 하기 위해 별도의 매칭 키 값을 인가하여야 하기 때문에 복잡한 테스트 시퀀스를 갖는다. [7]에서는 JTAG 표준 Test Access Port(TAP) 제어기의 스테이트머신에 새로운 스테이트를 추가하여 AES 정상 동작에서 스캔 테스트 동작으로 바뀔 방법으로 정상동작 시 남아있던 암호화 과정의 중간 값들이 스캔 테스트 방법으로 스캔 출력포트로 유출되는 것을 방지하기 위하여 반드시 파워-오프 동작을 거친 뒤 테스트 동작을 진행하도록 구현하여 TAP과의 호환성이 없게 되는 문제가 존재하게 된다. 또한 AES 코아 내부에 Mirror Key Register(MKR)을 추가하여 AES의 정상동작 시에는 사용자 키가 MKR로 로드되어 AES의 정상 동작을 위해 사용되어지며, 스캔테스트 동작 시에는 사용자 키가 AES코아로 인가되는 것을 방지하고 스캔입력 포트로부터 테스트 데이타가 MKR에 인가되어 AES를 테스트할 수 있도록 하였다. [7]의 방법은 AES내부에 MKR을 삽입하여 AES IP 코아의 수정을 요구하기 때문에 재사용 측면에서 단점을 가지고 있다.

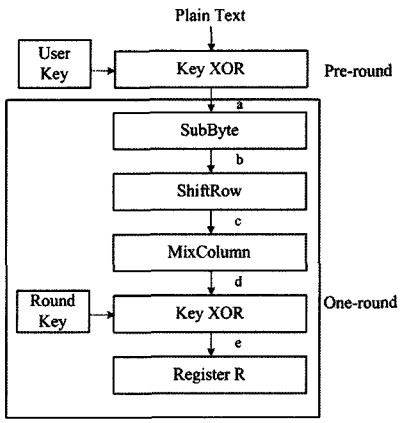

그림 1 AES 암호화 과정

3. 제안하는 시큐어 스캔 설계기술

그림 2는 스캔 기반 사이드 채널 공격에 의한 AES 키 정보 누출방지를 위해 본 논문에서 제안하는 시큐어 스캔 기술이 적용된 AES를 보여준다. JTAG에 스캔 테스트를 위한 TAP 명령을 추가하여 명령어 기반 방법

을 제안한다. AES가 정상 동작 모드에서 테스트 동작 모드로 바뀔 때 AES 내의 레지스터 값을 변경하기 위해 AES 코아의 외부에서 AES의 스캔체인에 연결된 MKR의 초기 값을 인가하여, AES를 정상동작 시킴으로써 [7]과는 다른 방법으로 내부의 레지스터 값을 변경시키는 방식을 사용하였다. 또한 [7]과 같이 AES 내부에 MKR를 추가하여 사용자 키와 테스트 데이타가 MKR에 인가되는 방법을 사용하지 않고 AES 외부에서 스캔체인에 연결하는 방식을 사용하여 AES IP 코아에 바로 적용이 가능하도록 구현을 하였다. [6]의 방법과 같이 스캔출력포트를 활성화시키기 위한 별도의 매칭키를 사용하지 않고 JTAG 명령어를 이용한 단순한 테스트 시퀀스를 제안하여 보다 쉽게 사용자 키 값이 누출되는 것을 방지하는 기술을 제시한다. 본 논문에서 제안하는 AES 코아 키 누출 방지 기술은 그림 2와 같이 AES 코아 내부 회로의 추가적인 수정 없이 적용이 가능하기 때문에 어플리케이션에 최적화 되어있는 AES IP를 수정할 필요가 없으므로 기존 방법과 비교하여 AES IP 코아의 재사용성을 높일 수 있다.

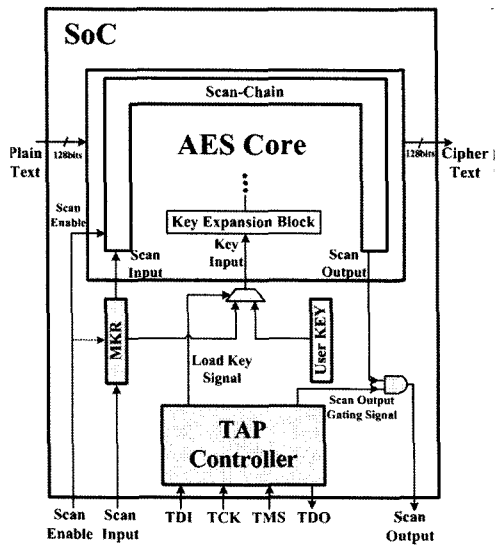

그림 2 AES 키 누출 방지를 위한 시큐어 스캔 구조

3.1 AES 정상 동작 모드에서 스캔 테스트 모드로 전환 시 AES 내부 레지스터 정보 변경 기술

AES 정상 동작에서 테스트 동작으로 변경 시 내부에 남아있는 데이타가 스캔 테스트 방법으로 노출이 되면 공격자의 표적이 될 수 있기 때문에 테스트 동작으로 변경되기 전에 AES 코아 내부의 레지스터 값을 변경시켜주는 기술이 필요하다.

이를 위해 본 논문에서는 JTAG 표준 TAP 제어기의 스테이트머신에 새로운 스테이트를 추가하여 파워-오프 동작을 거치도록 구현한 [7]과 달리 JTAG과의 호환성을 유지하기 위해 JTAG의 TAP 스테이트 머신에 변화를 주지 않고 JTAG에 스캔 테스트를 위한 TAP 명령을 추가하여 명령어 기반 방법으로 AES 정상 동작 모드에서 테스트 동작 모드로 바뀔 때 AES내의 레지스터 값을 변경 하도록 하였다. 제안하는 방식의 구체적인 내용은 다음과 같다. AES 정상 동작 모드에서 테스트 모드로 전환 시 그림 2와 같이 0으로 초기화되어 있는 MKR의 값이 TAP 제어기에서 보내어지는 Load Key 신호에 의해 사용자의 비밀 키 대신 AES에 인가되어 AES 내부 정보가 모두 변경될 때 까지 AES를 동작시키는 방법을 사용한다. 이때 AES 내부의 모든 레지스터의 값이 변경될 때 까지 스캔 체인 상의 값을 스캔 출력포트를 통해 볼 수 없어야 하므로 이를 위해 TAP 제어기에서는 그림 2에서와 같이 Scan Output Gating 신호를 사용하여 스캔 출력포트를 비활성화 시킨다. 또한 Scan Output Gating 신호는 정상동작 및 스캔 테스트 명령어가 TAP 제어기에 인가되기 전까지는 값이 0으로 유지되기 때문에 정상동작시 스캔 출력포트로 AES 코아의 내부 정보가 유출 될 가능성은 존재 하지 않게 된다. 본 논문에서 사용한 AES 코아는 그림 3과 같이 구현이 되어 있기 때문에 그림 4와 같이 2 클락 후 코아 내의 모든 레지스터가 키가 적용된 값으로 바뀐다. 그렇기 때문에 스캔 테스트를 위한 명령어 인가 후 TAP 제어기는 초기화 되어 있는 MKR의 0값을 사용자 키 대신 AES에 인가하여 Scan Output Gating 신호를 2 클락 동안 0으로 유지 후 1로 변경시켜 AES의 정상 동작 시 남아있던 정보들을 제거한 뒤 스캔 출력포트를 활성화 시킨다. 이렇게 AES 내부의 정상동작 시 남아 있던 정보가 2클락 후 제거되면 테스트 패턴을 인가하여 스캔 테스트를 정상적으로 하면 된다.

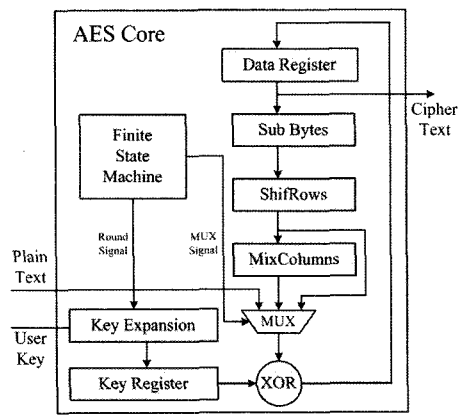

그림 3 AES 암호화 코아 설계 구조

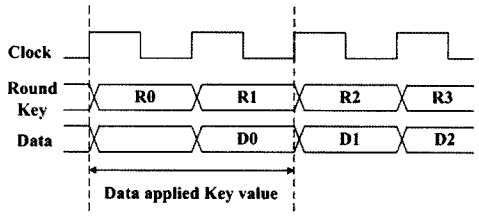

그림 4 AES의 Key 값이 적용되는 타이밍 다이어그램

본 논문에서는 사용하는 MKR 구조는 그림 5에서와 같이 크게 두 가지가 있다. 그림 5(a)는 멀티플렉스드 스캔 플립플롭을 사용하는 방법으로써, AES 정상 동작 시 또는 스캔 테스트 명령이 JTAG에 인가 된 후 2 클락 동안에는 플립플롭 데이타 입력 단에 0을 인가하여 MKR을 리셋시키는 방법이다. 그림 5(b)는 리셋이 있는 플립플롭 기반 방식으로써, AES 정상 동작에서 테스트 동작으로 변경되면 MKR을 TAP 컨트롤러에서 리셋 시켜 0으로 리셋된 MKR 값을 2 클락 동안 사용자 키 대신 AES에 인가되도록 하는 방법이다. 그림 5의 (a)와 (b) 두 가지 방법 중 선택의 기준은 설계 시 사용되는 공정 라이브러리의 리셋이 없는 스캔 플립플롭 셀과 리셋을 가진 플립플롭 셀의 크기와 전력소모를 고려하여 디자인에 적합한 방법을 선택 하면 된다. 본 논문에서 사용한 방법은 공정 라이브러리 상 작은 크기와 적은 전력소모를 갖는 그림 5(a)방법으로 구현 하였다. 본 논문에서 사용한 방법을 사용하면 AES 코아 내부의 플립플롭을 [7]처럼 리셋이 있는 플립플롭을 사용할 필요가 없어지게 되어 면적 오버헤드 및 전력 소모를 줄일 수 있게 된다.

3.2 스캔 테스트 동작 모드에서 사용자 비밀 키 누출 방지 기술

AES 코아의 스캔 테스트 시 사용자 비밀 키 누출을 방지 하면서 고장 검출율을 높이기 위해서는 테스트 모드 시 AES에 사용자 비밀 키 값을 대신한 데이타를 인가하는 기술이 필요하다. 이를 위해 본 논문에서는 그림 2에서와 같이 MKR을 AES 코아의 스캔 체인에 연결을 하고 스캔 테스트 시 MKR 레지스터로 스캔 테스트 데이타를 인가하도록 하였다. MKR에 인가된 스캔 테스트 데이타는 그림 2에서와 같이 TAP 제어기에서 보내지는 Load Key 신호를 통해 제어되는 멀티플렉서에 의해 사용자 비밀 키를 대신하여 AES에 인가된다. 이렇게 MKR을 통하여 스캔 테스트 시 AES 코아의 키 입력포트에 데이타를 인가하게 되면 Automatic Test Pattern Generator(ATPG)는 스캔체인의 일부로 속한 MKR을 포함하여 AES 스캔테스트를 위한 테스트 패턴을 생성한다. MKR로 인하여 AES에 인가할 수 있는 테스트 입력포트가 증가하여 AES의 테스트 제어도를 높일 수 있게 되어 고장 검출율을 다소 높일 수 있게 된다. 본 논문에서는 상업용으로 사용되는 Synopsys 사의 Tetra-Max라는 ATPG 툴을 사용하였다. MKR을 이용하여 AES의 키 입력포트에 입력된 데이타가 사용자 비밀 키와 같을 확률은 MKR의 길이가 n이라고 한다면 $1/2^n$ (n = 키의 길이, n >= 128)이기 때문에 사용자 키 노

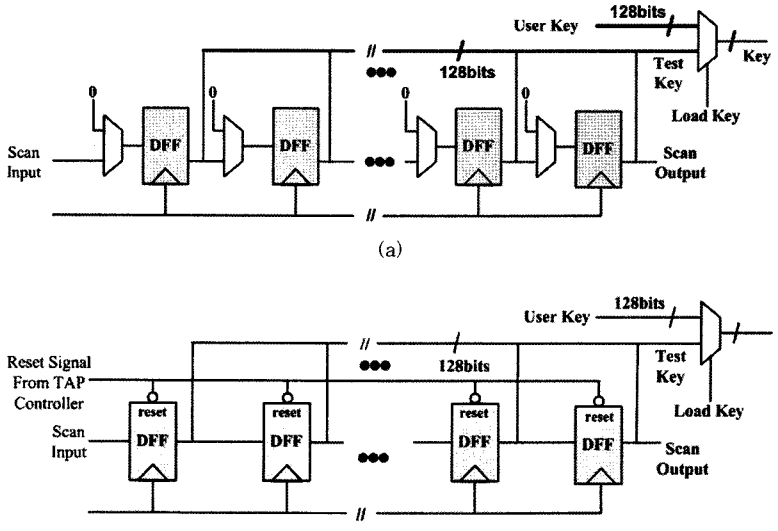

그림 5 제안하는 기술에 사용될 수 있는 MKR 구조 (a) 멀리플렉스드 스캔 플립플롭 기반 방식 (b) 리셋이 있는 플립플롭 기반 방식

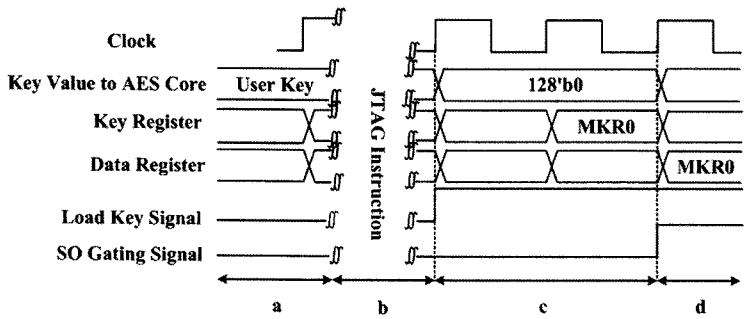

그림 6 AES 키 누출 방지를 위한 시큐어 스캔 타이밍도

출은 현실적으로 거의 불가능 하다는 것을 알 수 있다 [8]. 본 논문에서는 정상동작시 사용되지 않는 MKR로 인한 파워소모를 막기 위해 AES정상 동작 시 MKR이 클락 게이팅 되도록 하였다.

그림 6은 본 논문에서 제안한 방법을 절차적으로 나타낸 타이밍도이다. a에서 사용자 키 값을 사용하여 정상 동작하는 AES 코아에 b에서와 같이 JTAG 명령어를 인가한다. c에서 Load Key 신호가 1로 천이되면서 AES 코아는 MKR에 저장되어 있는 0값을 이용하여 내부의 레지스터 값이 모두 변경 되는 2클락 동안 정상동작을 하게 된다. AES의 정상동작시 남아있던 데이타들이 제거가 되면 SO Gating 신호를 통해 스캔출력포트가 활성화 된다. d에서부터 AES는 사용자 키 값을 사용하지 않으며 스캔체인에 연결된 MKR의 테스트 데이타 값을 이용하여 스캔 테스트를 정상적으로 할 수 있다.

4. 실험결과

표 1, 2, 3은 본 논문에서 제안한 방법을 평가하기 위해 면적 오버헤드, 정상 동작 시 전력소모 및 고장 검출율을 분석하여 논문[6,7]과 비교한 것을 보여준다. 본 실험에 사용된 AES는 1개의 스캔 체인을 갖으며 제안하는 기술과 비교 대상 논문 [6,7]은 JTAG 로직을 포함하고 있다. 본 실험을 위하여 모든 실험 대상들의 동작 주파수는 33MHz 클락 속도를 사용하였다. 객관적인 실험을 위해 모든 실험대상의 면적을 최소화 하는 방향으로 합성 조건을 설정하였다. 그리고 배치와 라우팅을 위해 다이의 크기는 1500×1500*um*로 고정을 하였으며 5층의 메탈 레이어를 사용하였다.

AES의 키 누출 방지를 위한 기술을 적용 후 정상 동작 시 추가되는 전력소모와 고장 검출율 측정을 위해서 상업용 전력소모 측정 툴과 자동 테스트 패턴 생성 툴을 사용하였다. 합성과 배치 및 라우팅은 MAGNA 0.18um 공정 라이브러리를 사용하였다. 표 1은 AES 코아에 기존 방식과 본 논문에서 제시하는 키 누출 방지 기술을 적용했을 경우의 면적 오버헤드를 보여준다. [6]의 M/N에서 M은 스캔 출력포트 활성화를 위한 매칭 키의 매칭 횟수를 나타내며 N은 매칭 키의 비트 길이를 나타낸다. 표 1을 통하여 본 논문에서 제안한 방법의 면적 오버헤드가 [7]보다 2.5% 적은 것을 볼 수 있으며, [6]에서 제시한 방법에서 매칭 키 비트의 길이가 증가하면 라우팅 오버헤드가 증가되기 때문에 본 논문에서 제시한 기술이 더 적은 면적 오버헤드를 갖을 수 있음을 M/N이 4/64 와 1/256인 경우를 통해 알 수 있다. 표 2는 AES 정상 동작 시 AES의 키 누출 방지 기술을 적용한 전력소모 오버헤드를 나타낸다. 본 논문은 MKR을 AES정상 동작 시 클락 게이팅 되도록 하였으며 AES 코아 내부에 [7]처럼 리셋이 있는 플립플롭을 사용할 필요가 없어지게 되어 전력 소모를 [7]보다 1.62% 줄였다.

표 1 면적 오버헤드 비교표

		Cell Area(um^2)	Routing Area(um^2)	Total Area(um^2)	Total Area Inc.(%)
AES		185221	215166	400387	Non
[7]		201786	219351	421137	5.18
[6] (M/N)	256/1	188948	215535	404483	1.02
	128/2	187624	215746	403370	0.75
	32/8	187647	217001	404648	1.06
	16/16	187467	219364	406831	1.61
	4/64	187920	223057	410977	2.64
	1/256	188212	227594	415806	3.85
Prop.		196035	215084	411119	2.68

표 2 노멀 동작 시 전력 오버헤드 비교표

		Dynamic Power(e-02)	Leakage Power(e-06)	Total Power(e-02)	Total Power Inc.(%)
AES		1.1272	5.285	1.1277	Non
[7]		1.1498	9.739	1.1508	2.04
[6] (M/N)	256/1	1.1301	5.464	1.1306	0.26
	128/2	1.1331	5.452	1.1336	0.52
	32/8	1.1397	5.434	1.1402	1.11
	16/16	1.1444	5.424	1.1449	1.53
	4/64	1.1538	5.407	1.1543	2.36
	1/256	1.1695	5.391	1.1700	3.75
Prop.		1.1317	7.742	1.1324	0.42

표 3 고장 검출율 비교표

		FC(%)	FC Inc.(%)	Scan Chain Length
AES		99.62	Non	262
[7]		99.68	0.06	390
[6] (M/N)	256/1	99.62	0	262
	128/2	99.62	0	262
	32/8	99.62	0	262
	16/16	99.62	0	262
	4/64	99.62	0	262
	1/256	99.62	0	262
Prop.		99.68	0.06	390

표 4 기존 기술과의 기술적 비교표

	AES	[6]	[7]	Prop.
Reuse of hard AES IP	Y	N	N	Y
Compatibility with JTAG	Y	Y	N	Y

[6]의 경우에는 스캔 플립플롭의 출력에 스캔 출력포트 활성화를 위한 매칭 블록으로의 연결선을 추가하기 때문에 N의 크기가 커질수록 팬아웃 부하가 증가하여 정상 동작 시 동적 전력소모가 증가된다. 결과적으로 본 논문에서 제시한 방법이 AES 정상 동작 수행 시 적은 전력소모 오버헤드를 갖는 것을 볼 수 있다. 표 3은 스캔 체인을 삽입한 AES 코아에 키 누출 방지를 위한 방법을 구현 했을 시 고장 검출율을 보여 주고 있다. 본 논문에서는 [7]과 같이 추가적인 MKR을 적용하여 스캔 체인의 길이는 증가되었지만 AES의 키 입력포트로 테스트 데이타를 입력 할 수 있기 때문에 [7]과 같이 테스트 제어도를 높일 수 있게 되어 [6] 보다는 다소 높은 고장 검출율을 보여준다.

본 논문에서 제시하는 방법은 면적과 파워 오버헤드의 비교를 통한 정량적 우수성 외에도, 기존 방법과 비교하여 기술적 우수성을 가지고 있다. 표 4에서 [6,7]과 본 논문에서 제안하는 방법을 기술적으로 비교를 하였다.

5. 결 론

본 논문에서는 MKR 및 JTAG 명령어 기반 기술을 사용하여 이미 소비자에 의해 사용되어지고 있는 SoC 상의 AES 암호화 코아의 스캔 기반 사이드 채널 공격에 대한 사용자 비밀 키 누출 방지를 위한 효과적인 방법을 제안하였다. 제안된 방식은 IEEE1149.1 표준 TAP 제어기와 호환성을 유지하며, 기존 방식보다 적은 면적 오버헤드와 전력 소모를 갖는 시큐어 스캔 기술임을 실험을 통해 알 수 있었다. 또한 어플리케이션에 최적화된 AES IP 코아를 사용 시 코아 자체의 추가적인 수정 없이 본 기술을 적용함으로써 키 누출을 방지할 수 있기 때문에 IP 코아의 재사용성을 높일 수 있다. 제안된 기술은 AES 뿐만 아니라, 사용자 키의 보호가 필요한 다른 암호화 코아에도 효과적으로 적용될 수 있을 것이다.

참 고 문 헌

[1] S. Mangard, M. Aigner and S. Dominikus, "A Highly Regular and Scalable AES Hardware Architecture," IEEE Transactions on Computer, Vol.52, No.1, pp. 483-491, April, 2004.

[2] D. Josephson and S. Poehhnan, "Debug methodology for the McKinley processor," International Test Conference, pp. 451-460, Baltimore, MD, USA, Oct. 30- Nov. 1, 2001.

[3] R. Kapoor, "Security vs. test quality: Are they mutually exclusive?" International Test Conference, pp. 1414, Charlotte, NC, USA, Oct. 26-28, 2004.

[4] J. Lee, M. Teharanipoor, and J. Plusquellic, "A Low-Cost Solution for Protecting IPs Against Scan-Based Side-Channel Attacks," VLSI Test Symposium, pp. 94-99, Berkeley, CA, USA, Apr. 30-May 4, 2006.

[5] B. Yang, K. Wu and R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard," International Test Conference, pp. 339-344, Charlotte, NC, USA, Oct. 26-28, 2004.

[6] S. Paul, R. S. Chakraborty and S. Bhunia, "VIm-Scan : A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips," VLSI Test Symposium, pp.

455-460, Berkeley, CA, USA, May 6-10, 2007.
[7] B. Yang, K. Wu and R. Karri"Secure Scan : A Design-for-Test Architecture for Crypto Chips," IEEE Transaction Computer-Aided Design of Integrated Circuits and systems, Vol.25, No.10, pp. 2287-2293, Oct. 2006.
[8] W. Stallings, "Cryptography and Network Security," Englewood Cliffs, NJ : Prentice-Hall, 2003.

송 재 훈
2000년 한양대학교 전자컴퓨터공학과 학사 졸업. 2002년 한양대학교 컴퓨터공학과 석사 졸업. 2003년 서울대학교 SoC 설계 센터 연구원. 2004년~현재 한양대학교 컴퓨터공학과 박사 재학중

정 태 진
2007년 한양대학교 컴퓨터공학과 학사 졸업. 2007년~현재 한양대학교 컴퓨터공학과 석사 재학중

박 성 주
1983년 한양대학교 전자공학과 학사 졸업. 1983년~1986년 금성사 소프트 웨어 개발 연구원. 1992년 Univ. of Massachusetts 전기 및 컴퓨터공학과 박사 졸업 1992년~1994년 IBM Microelectronics 연구스텝. 1994년~현재 한양대학교 전자컴퓨터공학부 정교수