정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

CHES 2020로 살펴본 부채널 분석 보안 컨퍼런스 연구 동향

김 한 빛*, 김 희 석**

요 약

CHES는 암호 알고리즘의 하드웨어/소프트웨어 구현의 설계 및 분석에 대한 다양한 성과가 발표되는 부채널 분석 분야 최대 규모의 보안 컨퍼런스이다. 본 기고는 CHES 컨퍼런스에 발표된 논문들에 대하여 부채널 공격 관점, 부채널 대응 및 구현 관점, CHES에서 주제로 다루는 암호 알고리즘의 추이 관점으로 구분하여 동향을 분석한다. 이를 위하여 오류주입 공격, 머신러닝 기반 부채널 공격, 캐시공격, 부채널 누출 검증 방법론과 부채널 역공학 기술 등 다양한 부채널 공격을 소개하고 최신 논문 주제의 흐름에 대하여 논의한다. 또한, 소프트웨어 고차 마스킹과 하드웨어 TI, PUF/난수 발생기 등의 부채널 대응기술 및 구현 동향을 분석하며, CHES에 발표된 논문들이 주제로 다루는 대칭키, 공개키 암호 및 화이트박스 암호 추이를 분석한다. 이러한 CHES 컨퍼런스의 주제별 연구 동향 분석 결과는 부채널 분석 연구자에게 유용한 정보를 제공하고 향후 연구 방향에 대한 중요한 지표가 될 수 있을 것이다.

Ⅰ. 서 론

최근 정보통신 이용자의 폭발적인 증가와 다양한 네트워크, 통신 인프라의 발전으로 통신 서비스에 대한 이용자의 요구가 고도화/다양화되고 있다. 이러한 요구를 만족하고자 정보보호 기술, 정보통신 기술의 향상을 위한 연구 개발이 세계적으로 활발하게 이루어지고 있으며, 기술의 고도화를 지지하기 위한 보안 소프트웨어 및 하드웨어 기술의 연구 개발이 활발하게 진행되고 있다. 특히 IC 카드 및 보안토큰, ATM기, 보안 라우터 등과 같은 소프트웨어 및 하드웨어 기반의 보안 시스템에 양질의 보안 서비스를 제공하기 위한 암호 연구 및 표준화 작업이 활발하게 진행되고 있다.

암호 시스템에 대한 기존의 안전성 평가는 증명 가능한 안전성이나 계산적 안정성과 같은 이론에 기반을 두고 있다. 그러나 최근 암호 시스템이 구현된 하드웨어에 대한 또 다른 형태의 공격이 제기되고 있어 암호 시스템의 실질적인 안전성 평가가 중요한 쟁점으로 떠오르고 있다. 스마트카드, 모바일 폰, PDA 등과 같은 보안 장치에서 암호 알고리즘이 구현될 때, 전력 소모량, 알고리즘의 수행 시간 및 전자파 방출량 등과 같은 비밀키에 관련된 부가 정보가 공격자에게 악의적으로 이용될 수 있다. 암호 시스템에 대한 이러한 형태의 공격을 부채널 공격(Side Channel Analysis, SCA)이라고 한다[1]. 부채널 공격은 1996년 Paul Kocher에 의해 암호 프리미티브에 대한 시간 공격(Timing Attack)[2] 소개를 시작으로, 1999년에 전력 분석(Power Analysis)의 개념이 소개되면서 본격적으로 연구되기 시작하였다[3,4].

부채널 공격에 대응하기 위한 기술은 알고리즘적인 대책과 물리적인 대책으로 강구될 수 있다[5]. 부채널 공격은 비밀정보와 암호 알고리즘 수행의 연관성을 이용한다. 제안된 부채널 공격이 가능하기 위해서는 여러 가지 공격의 모델링 및 추측 가정이 필요하다. 만약 민감한 정보를 암호화하는 스마트카드의 전력 소모 모델링 또는 중간값 추측 가정을 어렵게 스마트카드를 설계할 수 있다면, 부채널 공격을 원천적으로 봉쇄하는 방법이 될 수 있다. 암호 알고리즘이 장착된 하드웨어 및 소프트웨어 장비에서 신뢰할 수 있는 보안 서비스를 제공하려면 부채널 공격 기술에 대한 이해와 이를 대비하기

이 성과는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구 재단의 지원을 받아 수행된 연구임(No.NRF-2019R1A2C2088960).
* 고려대학교 정보보호대학원 정보보호학과, 고려대학교 정보보호연구원 (연구원, luzdamoon@korea.ac.kr)
** 고려대학교 인공지능사이버보안학과 (부교수, 80khs@korea.ac.kr)

〔그림 1〕 CHES 2018부터 2020까지 출간된 논문을 이용하여 구성한 단어구름

위한 암호 알고리즘의 개발이 필수적이다[6].

1999년부터 매년 개최되는 CHES (Cryptographic Hardware and Embedded Systems)는 암호 알고리즘의 하드웨어/소프트웨어 구현의 설계 및 분석에 대한 새로운 성과들을 다양한 결과물로 발표하고, 이를 통하여 연구자들과 기업 및 정부 기관 사이에 다리를 연결하는 중대한 소임을 수행하고 있는 부채널 분석 분야 최대 규모의 보안 컨퍼런스이다[1]. [그림 1]은 CHES 2018부터 2020까지 출간된 논문을 이용하여 구성한 단어구름이다. 이를 통하여 CHES에서 관심 있어 하는 키워드를 파악해볼 수 있다. CHES에서 주로 다루는 주제는 간략하게 암호 구현, 구현물 및 대응기술에 대한 공격, 신규 암호 알고리즘 및 프레임워크 등이 있으며, 최근 머신러닝 분야와 적극적인 교류를 하며 다양한 분야로 확장을 시도하고 있다. 2018년에는 더 좋은 출판 환경을 위하여 오픈 엑세스 저널/컨퍼런스 하이브리드 모델인 TCHES (IACR Transactions on Cryptographic Hardware and Embedded Systems)로 학회명을 변경하고, 3개월마다 논문을 제출할 수 있어 승인논문의 질적 상향을 도모하고 있다.

CHES에서 주로 다루는 논문 주제를 정리하면 다음과 같다.

- 암호 구현
  - 하드웨어 구조 설계
  - 암호 연산 가속기 프로세서
  - 트루/의사 난수 생성기
  - 물리적 복제 불가능 함수 (PUF)
  - 효율적인 소프트웨어 암호 구현
- 구현물 및 대응기술에 대한 부채널 공격
  - 신규 부채널 공격 및 대응기술
  - 오류주입 공격 및 대응기술
  - 하드웨어 변조(tampering) 및 탐지기술
  - 화이트 박스 암호 및 코드 난독화
  - 하드웨어 및 소프트웨어 역공학
- 분석 도구 및 방법론
  - 효율적인 전수조사 기법
  - 부채널 안전성 검증 및 도구
  - 임베디드 시스템의 부채널 안전성 평가 도구
  - 시큐어 코딩/프로그래밍 기술
  - FPGA 보안 설계
  - 안전한 하드웨어 및 소프트웨어 정형화 기법 (Formal method)
- 안전한 암호 이론 및 구현
  - 소형 장치를 위한 새로운 암호 알고리즘 및 프로토콜
  - 부채널 및 암호 분석을 위한 전용 하드웨어 설계

1) CHES URL : https://ches.iacr.org

- 부채널 신호 누출 탐지 및 내성 설계

• 적용 분야
- 사물인터넷(RFID, 센서 네트워크, 스마트 기기, 스마트 미터 등)을 위한 암호 알고리즘
- 하드웨어 IP 보호 및 위조 방지
- 재구성 가능한(Reconfigurable) 하드웨어를 위한 암호 알고리즘
- 스마트카드의 프로세서, 시스템, 및 애플리케이션
- 사이버 물리 보안을 위한 보안
- 자동차 보안
- 안전한 저장장치 보안
- 지식재산 콘텐츠 보호를 위한 기술
- 신뢰할 수 있는 컴퓨팅 연산

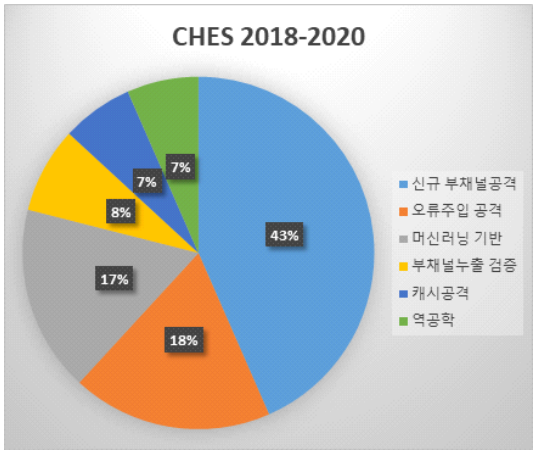
본 기고는 최근 3년 동안 CHES에서 발표된 논문 동향을 조사·분석한다. TCHES로 전환한 2018년부터 가장 최근에 인터넷 출간된 2020년 네 번째 이슈까지 3년 동안 출판된 총 논문 편수는 149편이다. 본 기고는 연구 동향을 더 구체적으로 조사하기 위하여 학회에서 다루는 연구 분야에 따라 논문을 정리 및 분류하고, 해당 주제마다 동향을 분석한다. 먼저 출간논문의 성향이 부채널 공격 관점에서 주로 서술되는지, 대응기술 및 대응기술이 적용된 암호 알고리즘의 최적화 구현 또는 특수 환경에 암호 최적화 구현 관점에서 논문이 서술되는지에 따라 범주를 나누었다. 부채널 공격과 대응기술은 각각의 목표가 명확하게 대조되고, 거의 모든 논문이 두 범주로 분류될 수 있다. 여기서 대응기술 이슈와 구현 이슈를 함께 묶은 이유는 최근에 발표되는 논문들은 기본적으로 부채널 대응기술이 적용된 암호 알고리즘을 구현하는 경우가 대부분이기 때문이다. 분류 결과 부채널 공격은 총 76편, 부채널 대응기술 및 구현은 총 80편이다. 이 중 7편은 신규 부채널 공격 소개 및 제안하는 공격을 막기 위한 대응까지 제시한 경우이다. 또한, 본 기고에서는 CHES에서 발표된 논문들이 주제로 다루는 암호 알고리즘의 추이를 조사 및 분석하였다. 이러한 추이 분석은 각각의 암호 알고리즘 종류마다 최신의 부채널 공격 및 대응기술 개발에 주요 쟁점이 무엇이고, 미진한 부분은 어디인지에 대하여 가늠해 볼 수 있는 정보를 제공할 수 있을 것이다. 앞선 내용을 정리하면 다음과 같다. 본 기고는 학회 동향을 크게 세 가지 관점에서 분석하고 결론을 맺고자 한다. 첫째는 CHES에서 가장 비중 있게 다루고 있는 부채널 공격 관점에서 동향을 분석한다. 신규 부채널 공격 중 주목해 볼 만한 내용을 소개하고, 오류주입 공격, 머신러닝 기반 부채널 공격, 캐시공격, 부채널 누출 검증 방법론과 부채널 분야에서의 역공학을 설명한다. 둘째는 부채널 대응기술과 부채널 분야에서 구현 이슈에 대하여 알아본다. 암호 알고리즘 및 대응기술의 적용과 해당 암호의 고속화 구현 현황에 대하여 논의하고, PUF/난수 발생기와 관련된 연구를 소개한다. 추가로 부채널 대응기술 연구 동향은 더 세밀하게 분류하여 소프트웨어에서 부채널 공격에 안전하다고 알려진 고차 마스킹 기법과 하드웨어서 안전하다고 알려진 TI(Threshold implementation)를 알아본다. 다음으로 부채널 공격, 대응기술 및 구현의 적용 대상이 되는 다양한 암호 알고리즘의 동향을 분석한다. 널리 알려진 AES와 같은 대칭키 암호 및 RSA와 ECC 같은 공개키 암호를 비롯하여 최근 양자 컴퓨터의 발전으로 계속해서 관심이 집중되는 후양자 암호에 대하여 부채널 분석 및 대응기술의 연구 동향을 알아본다. 이외에 특수한 소프트웨어 환경을 위하여 설계된 화이트 박스에 관한 부채널 연구 동향을 정리한다. 마지막으로 앞서 조사 및 분석한 내용을 정리하며 결론을 맺는다.

Ⅱ. 부채널 공격 연구 동향

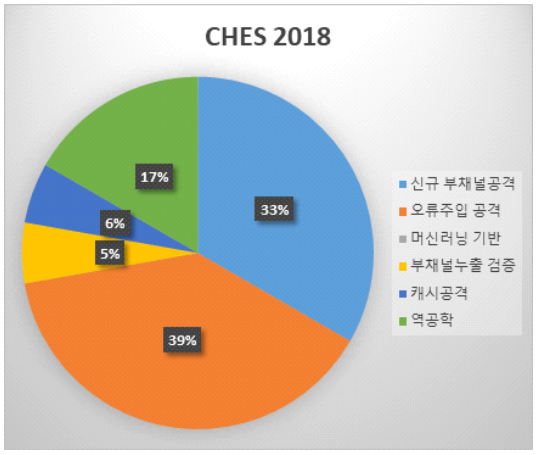
본 장에서는 최근 CHES에 발표된 부채널 공격과 관련된 논문에 대하여 논의한다. [그림 2-5]와 [표 1]은 2018년도부터 3년 동안 CHES에서 발표된 논문 중 부채널 공격에 중점을 둔 논문의 편수이다. 기본적으로 새로운 암호 알고리즘 및 대응기술과 구현물을 대상으로 하는 새로운 부채널 공격은 항상 주목받는 소재임이 틀림없다. 오류주입 역시 꾸준히 연구되는 주제이다. 주목해 볼 점은 2018년도에 한 편도 없었던 머신러닝 기반

〔표 1〕 최근 3년 CHES 발표 논문 (부채널 공격)

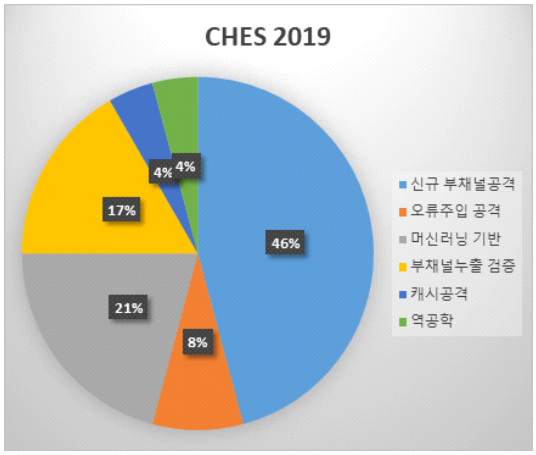
종류	2018년도	2019년도	2020년도
신규 부채널 공격	6	11	16
오류주입 공격	7	2	5
머신러닝 기반 공격	0	5	8
캐시 공격	1	1	3
부채널 누출 검증	1	4	1
부채널 역공학	3	1	1



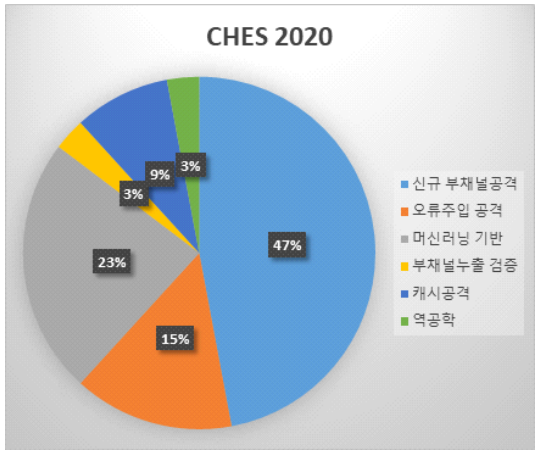
〔그림 2〕 부채널 공격 연구 분야 (CHES 2018-2020)



〔그림 3〕 부채널 공격 연구 분야 (CHES 2018)



〔그림 4〕 부채널 공격 연구 분야 (CHES 2019)



〔그림 5〕 부채널 공격 연구 분야 (CHES 2020)

부채널 공격이 2019년과 2020년에 폭발적으로 증가한 것이다. 이는 딥러닝 분야의 관심이 증가한 결과라고 할 수 있다. 따라오는 절에서는 각각 소분야 대한 간략한 정리와 주목해 볼 논문을 소개한다. 신규 부채널 공격 분야에서는 실제 유통되고 있는 암호 장비를 대상으로 부채널 공격을 수행한 사례에 대하여 중점적으로 알아본다. 다음으로 오류주입 공격, 머신러닝 기반 부채널 공격, 캐시 공격과 관련된 최신 동향을 소개한다. 추가로 부채널 공격에 유용한 정보로 활용되거나 부채널 평가 관점에서 주목받고 있는 부채널 누출 검증 기술에 대하여 논의하고, 마지막으로 부채널 분야에서 역공학 관점을 담당하고 있는 하드웨어 트로이에 대하여 알아본다.

2.1. 신규 부채널 공격 연구 동향

새로운 암호 알고리즘이 제안되거나 강력한 부채널 대응기술이 소개되면 부채널 연구자들은 이를 무력화 시키기 위하여 다양한 시도를 준비한다. 대표적인 주제를 살펴보면 다음과 같다. 2019년과 2020년에 발표된 시중에 유통되고 있는 스마트 자동차를 대상으로 하는 공격 논문은 부채널 공격자가 얼마나 현실적인 위협 요소로 발전하였는지 가늠할 수 있는 자료이다[7,8]. 이 논문은 스마트 자동차 키 팝(key fob)에 사용되는 비공개 암호 알고리즘의 보안취약점을 이용하여 스마트 차량 시스템 전체를 해킹하는 공격을 시연하였다. 이 과정에서 부채널 공격 기술뿐만 아니라 디케핑, 역공학, 통신 도청, 암호 취약점 분석, 키 전수조사 등의 암호 분

야 전반의 모든 기술을 망라하였으며, 이러한 일련의 과정에서 부채널 공격의 중요성과 부채널 공격이 단지 이론에서 머물지 않고 현실로 반영될 수 있는 다양한 시나리오를 소개하였다.

2.2. 오류주입 공격 연구 동향

오류주입 공격은 레이저 및 강한 전자기파를 방출하여 회로에 직접 오동작을 유도하는 방법뿐만 아니라, 전압을 갑자기 떨어트리거나 올리거나 하는 전압 가변 방식, 장치의 동작 주파수에 변화를 주는 클록 가변 방식 등 다양한 방식의 오류가 암호 알고리즘에 주입되었을 때 발생하는 오동작(명령어 생략, 비트플립 등)을 분석하여 비밀정보를 갈취하는 공격 기법이다. 이와 같은 다양한 오류 종류, 오동작 모델이 있는 오류주입 공격 중에 CHES는 로우해머(rowhammer) 공격에 주목하고 있다. 2014년도에 처음 제안된 로우해머 공격은 DRAM 칩 안에 있는 메모리 셀이 용량과 효율성 문제 때문에 매우 가까이 붙어 있고, 이러한 물리적 구조의 한계로 메모리 한 열에 반복적인 접근을 수행할 때 인접한 메모리 비트의 플립이 일어나는 현상으로 비밀정보를 갈취하는 공격이다. CHES에서는 FPGA 등의 각각의 하드웨어마다 특징적으로 발생하는 로우해머 현상을 좀 더 명확하게 설명하는 연구에서부터[9,10], 실제 블록암호가 구현된 FPGA에 대하여 로우해머 공격을 수행하고 비밀키를 찾는 공격과 같은 연구가 활발히 논의되고 있다[11].

2.3. 머신러닝 기반 부채널 공격 연구 동향

머신러닝 기반 부채널 공격 분야는 2018년 이전에는 CHES에서 그리 활발하게 토론이 이루어지는 분야는 아니었다. 그러나 딥러닝이라는 새로운 머신러닝 분야가 대두됨에 따라 CHES에서도 매우 뜨거운 이슈로 자리매김하게 되었다. 딥러닝은 머신러닝의 한 종류로 20세기 중반부터 연구가 시작된 기술이다. 하지만 컴퓨팅 환경의 부재, 데이터 부족 등의 이유로 다른 머신러닝보다 좋은 성능을 내지 못하고 있었으나 21세기 초부터 딥러닝 알고리즘의 발달과 빅데이터 시대, 그리고 클라우드 등 컴퓨팅 파워의 발달과 함께 딥러닝 기술의 성능이 급속히 증가하여 영상 처리, 자연어 처리, 기계번역, 질병 진단 등 다양한 분야에서 좋은 성능을 보인다[12].

CHES에서 발표된 초기 머신러닝 기반 부채널 공격 연구는 학습 데이터가 주어진 프로파일링 공격의 관점에서 공격 성능을 향상하기 위한 연구가 주를 이루었다. 딥러닝 기반 프로파일링 공격은 분석 대상의 전력 소모 파형을 학습 데이터로, 비밀연산의 중간값을 라벨로 사용하여 신경망을 학습하고, 학습된 네트워크를 이용하여 비밀정보를 갈취한다. 그 결과 부채널 프로파일링 공격 분야에서 널리 사용되어온 템플릿 공격과 비교하여 더 좋은 성능을 가짐을 실험을 통하여 확인하였다. 공격의 대상 역시 대응기술이 미적용되거나 약한 대응기술이 적용된 대칭키 암호 알고리즘 위주로 진행되었다. 그러나 최근에 오면서 대표적인 부채널 대응기술인 마스킹 및 하이딩 기법이 적용된 대칭키 암호를 대상으로 딥러닝 기반 부채널 공격의 가능성을 보임을 시작으로[13,14], RSA와 같은 공개키 암호에 대하여 공격이 수행되고, 부채널 테스트 보드가 아닌 EAL4+인증을 통과한 카드 타입의 상용 장비에 대하여 머신러닝 기반 부채널 분석을 수행한 논문이 발표되고 있다[15]. 단순하게 프로파일링 공격의 도구로 머신러닝이 쓰이는 것이 아닌, 논프로파일링 공격으로 학습 데이터 없이 비밀키를 찾는 연구가 진행되었으며[16], 부채널 공격에 최적화된 손실함수 및 앙상블 모델 연구가 활발하게 논의되고 있다[17,18].

2.4. 캐시공격 연구 동향

Meltdown, Spectre로 대표되는 캐시공격은 부채널 공격의 한 종류로 소비 전력, 전자파 등을 분석하는 기존의 부채널 공격과는 대조적으로 캐시의 상태 변화를 관찰하여 데이터를 유출한다[19]. 부채널 분야에서 캐시공격은 꽤 오래전부터 연구가 진행되었으며, 대표적인 Flush + Reload 공격은 캐시에 적재된 데이터와 그렇지 않은 데이터에 접근할 때 각각의 접근 속도에 차이가 있다는 점을 이용한 공격 방법이다[20]. 희생자가 접근한 데이터는 이미 캐시에 적재되어 있어 공격자가 다시 접근할 때 접근 속도가 매우 빠르지만, 희생자가 접근하지 않았던 데이터라면 접근 속도가 전자의 경우보다 훨씬 느리므로 공격자는 희생자의 데이터 접근 여부를 확인할 수 있다. 캐시공격은 운영체제의 CPU 종

류에 따른 특화된 분석방법이 존재한다. CHES에서 주요 공격 대상이 되는 CPU는 Intel 사의 SGX 보안 기능이 추가된 프로세서이다. SGX는 신뢰성 있는 연산(Trusted execution)을 위한 하드웨어로, 사용자 응용 소프트웨어가 실행되는 코드와 데이터 영역의 메모리를 암호화함으로써 응용 프로그램의 기밀성 제공 및 하드웨어 공격 또는 악성 운영체제로부터 응용 프로그램을 보호하는 기술이다. CHES에 발표된 논문은 이러한 SGX 프로세서에서 동작하는 공개키 암호 알고리즘을 대상으로 캐시공격을 수행하여 비밀키를 갈취하는 방법을 제시한다[21,22].

2.5. 부채널 누출 검증 연구 동향

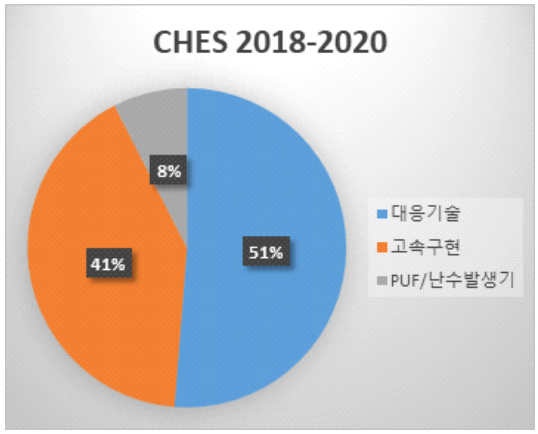
부채널 정보 누출에 대한 정량화는 암호 모듈 검증제도와 CC 평가 등에서 암호 시스템이 측정해야 하는 보안 요구사항 중 하나이다[23]. 부채널 신호에 부가 정보가 담겨 있는지 분석하는 부채널 누출 검증 연구는 이러한 검증제도에 대비하기 위하여 부채널 대응기술이 잘 동작하고 있는지 확인할 수 있는 척도가 될 수 있으며, 공격자 관점에서는 시간 도메인의 부채널 파형 중 어느 부분에서 정보 누출이 발생하는지 파악하여 공격 복잡도를 낮추는 도구로 활용될 수 있다. 가장 대표적인 부채널 누출 검증 도구는 TVLA(Test Vector Leakage Assessment)로 2011년 처음 발표되었고, 이후 CHES에서는 TVLA의 성능을 더 향상하기 위한 다양한 제안이 발표되고 있다[24-26].

2.6. 부채널 역공학 연구 동향

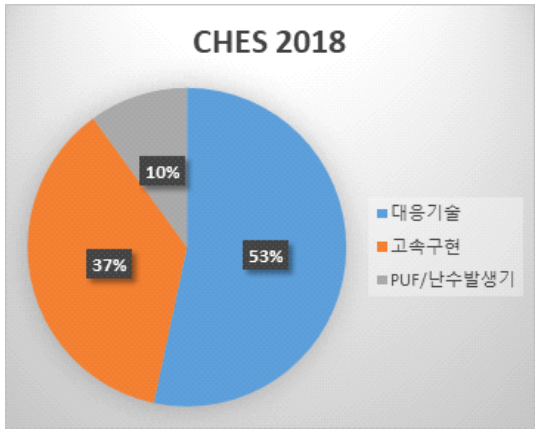
일반적으로 알려진 역공학이란 기기에서 소프트웨어 또는 하드웨어가 동작하는 내부 연산 과정을 정적/동적 구조분석을 통해 발견하는 기술이다. 또한, 시스템의 유지 보수를 위해 대상의 세부적인 작동을 분석하는 것을 포함한다. 부채널 분야에서 역공학 연구는 후자로 하드웨어 트로이를 검출하는 것을 주목적이 있다[27]. 하드웨어 트로이란 예를 들어 사물인터넷의 소형기기 내부에 장착된 IC의 뒷면이나 회로기판에 악의적으로 설치한 미세한 통신 칩을 가리키는데, 사이버 공격의 근거로 이용하거나 정보를 빼내는 게 목적이며, 소프트웨어 악성코드의 하드웨어 버전이라고 할 수 있다. 이러한 하드웨어 트로이는 대부분 완성된 회로기판에 나중에 장착되는 형태로 배포되는데, CHES에서는 링오실레이터 등의 기술을 이용하여 하드웨어 트로이가 추가로 사용하는 전원 및 교환되는 전기신호를 감지하여 비밀정보의 누출을 차단하는 연구에 관심이 있다[28,29].

Ⅲ. 부채널 대응 및 구현기술 연구 동향

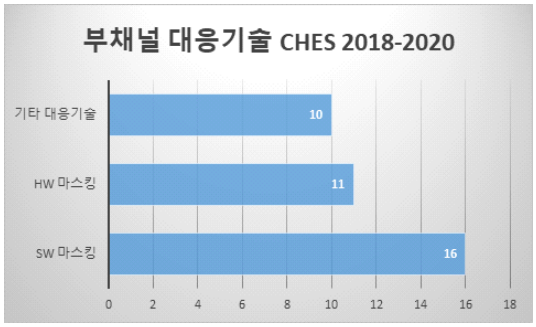
본 장에서는 최근 CHES에 발표된 부채널 대응기술 및 알고리즘 구현과 관련된 논문에 대하여 논의한다. [그림 6-10]과 [표 2]는 2018년도부터 3년 동안 CHES에서 발표된 논문 중 부채널 대응기술과 알고리즘 구현 결과에 중점을 둔 논문의 편수이다. 부채널 대응기술은 공격 기법과 더불어 부채널 연구 분야를 이끄는 핵심축 중 하나이다. 비록 공격과 비교하면 이에 대응하기 위한



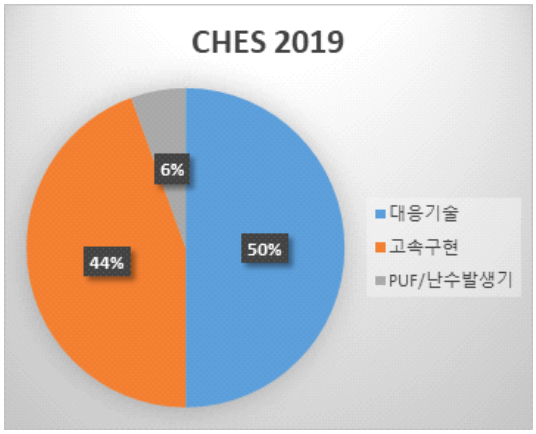
〔그림 6〕 부채널 대응 및 구현 분야 (CHES 2018-2020)



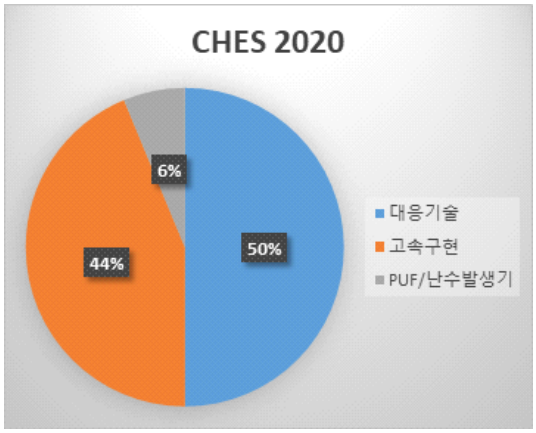
〔그림 7〕 부채널 대응 및 구현 분야 (CHES 2018)



〔그림 8〕 부채널 대응기술 분야 (CHES 2018-2020)



〔그림 9〕 부채널 대응 및 구현 분야 (CHES 2019)



〔그림 10〕 부채널 대응 및 구현 분야 (CHES 2020)

논리를 설계하고 안전성을 검증하는 과정이 매우 어렵지만, 꾸준히, 그리고 다양한 시각에서 부채널 대응기술 관련 논문은 제안되고 앞으로도 제안될 것이다. 구슬이 서 말이라도 꿰어야 보배라는 속담이 있듯 구현기술 역

〔표 2〕 최근 3년 CHES 발표 논문 (부채널 대응 및 구현)

종류	2018년도	2019년도	2020년도
부채널 대응기술	16	9	16
부채널 고속구현	11	8	14
PUF/난수 발생기	3	1	2

시 매우 중요하다. 특히 단순한 속도 최적화 구현뿐만 아니라 메모리가 풍요로운 또는 부족한, 프리미티브 연산 가속기가 내장된 특수한 환경 등과 같은 주어진 컴퓨팅 자원하에서 최적화 구현 연구는 하드웨어가 발달함에 따라 지속해서 제안되고 종전의 신기록을 경신해 나가고 있다. 이후 절에서는 부채널 대응기술 연구 동향과 대응기술에 두 개의 주축인 소프트웨어 기반 고차 마스킹과 하드웨어 기반 TI 마스킹 기법에 관하여 서술하고, 대응기술의 구현결과물 및 특수 환경에서의 고속화 구현과 관련된 동향을 알아본다. 추가로 신규 PUF에 대한 설계 및 취약점 분석과 PUF를 이용한 난수 발생기의 동향을 조사한다.

3.1. 부채널 대응기술 연구 동향

다양하고 강력한 부채널 공격이 CHES에 소개되면서 그를 막을 수 있는 부채널 대응기술도 다양한 방식으로 제안된다. 그중 암호 알고리즘의 연산이 수행되는 도중 중간값의 정보를 숨겨 정보의 누출을 막는 마스킹 기법과 연산을 추가하거나 하드웨어를 조정하여 SNR(Signal-to-Noise Ratio)을 증가시키는 하이딩 기법이 CHES에서 주로 다루어지는 주제이다[30,31]. [표 3]은 최근 3년 동안 CHES에서 발표된 부채널 대응기술과 관련된 논문 편수이다. 본 절에서는 다양한 대응기술 중에 가장 활발하게 연구되고 있는 소프트웨어 및 하드웨어 기반 마스킹 기법에 대하여 중점적으로 다루겠다.

〔표 3〕 최근 3년 CHES 발표 논문 (부채널 대응기술)

종류	2018년도	2019년도	2020년도
SW 마스킹	8	2	4
HW 마스킹	6	4	1
기타 대응기술	2	3	5

3.1.1. 소프트웨어 기반 마스킹 기법 연구 동향

소프트웨어에서 마스킹 기술은 모든 암호 연산의 중간값을 랜덤한 난수로 숨기는 방법을 의미한다. 난수로 중간값을 숨기면, 이를 추측할 수 없으므로 일반적인 전력분석 공격은 성공할 수 없다. 마스킹 방법의 종류로는 산술 마스킹과 불 마스킹이 있다. 산술 마스킹이란 마스킹 난수가 산술 덧셈, 뺄셈, 곱셈으로 연산 되어있는 경우이고, 불 마스킹은 마스킹 난수가 XOR 되어있다. 하지만 마스킹 대응기술은 비밀정보의 분할(secret sharing) 개수보다 더 많은 측정이 가능한 d-probing 공격자에 취약하다. 이에 대응하기 위한 고차 마스킹 대응기술은 비밀정보를 (d+1)개 이상으로 나누어 암호 연산을 수행하도록 알고리즘을 구성하고, 그 결과 서로 다른 시점에 비밀정보와 관련된 부채널 신호가 나누어져 있게 되어 d-probing 공격자에 대하여 부채널 안전성을 제공한다[32]. 그러나 고차 마스킹 기법은 비밀정보의 분할 개수에 따라 마스킹 비선형 연산에 추가되는 비용이 급격하게 커지는 경향을 보인다. CHES에서 최근 다루는 소프트웨어 기반 고차 마스킹 기법은 ISW 프레임워크에 기반한 d-probing 공격자에게 안전한 구현물을 메모리, 소요시간, 필요로 하는 난수의 비트 측면에서 더욱 효율적으로 구현하는 방법론과[33,34], 격자 또는 코드 기반의 후양자 암호와 같은 비교적 암호 프리미티브 연산이 간단한 공개키 암호에 마스킹을 적용하는 연구가 주를 이루고 있다[35-37].

3.1.2. 하드웨어 기반 마스킹 기법 연구 동향

같은 마스킹 기법이라 하더라도 소프트웨어 기반의 고차 마스킹 기법과는 다르게 하드웨어 기반 마스킹 기법은 글리치(glitch) 공격에 안전하도록 설계된 TI (Threshold Implementation) 기법이 활발히 연구되고 있다[38]. TI 기법에 대하여 알기 위해서는 하드웨어에서만 발생하는 글리치 공격을 살펴볼 필요가 있다. 마스킹 기법은 게이트의 모든 입력 신호(비트 정보)는 동시에 게이트에 도착한다는 이상적인 환경(소프트웨어 구현)의 가정에서 부채널 안전성이 보장된다. 그러나 현실, 특히 하드웨어 구현 관점에서 게이트의 입력 신호는 여러 가지 이유로 서로 다른 시간에 도착한다. 예를 들어 신호가 게이트를 통과하게 되면 게이트 지연 시간이 발생할 수 있고 또한 신호가 거쳐야 하는 거리에 따라 역시 게이트 도달 시간이 다를 수 있다. 입력 신호가 서로 다른 시간에 게이트에 도착하게 되면 해당 게이트의 출력값은 한 클록 사이클 내에서 안정화되기 전까지 여러 번 변하게 되는데 이러한 현상을 글리치라고 하고, 글리치 현상과 전력소비량 사이의 관계를 이용하여 암호 기기 내에 저장된 비밀정보를 알아내는 전력분석 공격법을 글리치 공격이라고 한다. TI 기법은 글리치 공격에 안전하도록 하드웨어를 설계하는 기술로, 한 클록의 연산에서 correctness, non-completeness, uniformness라는 3가지 특성을 만족하도록 하드웨어 회로를 구성한다. 간략하게 correctness는 마스킹 회로에서 분할된 정보의 입력들로 계산된 출력들은 본래 회로의 연산 출력과 같은 정보를 가져야 한다는 성질이다. Non-completeness는 분할된 비밀정보 중 적어도 하나는 마스킹 회로의 입력으로 사용되면 안 된다는 성질이다. 마지막 uniformness는 마스킹 회로의 출력 확률 분포는 본래 회로의 출력 확률 분포와 같은 분포를 형성해야 한다는 성질이다. TI 기법 역시 소프트웨어 기반 고차 마스킹 기법과 같이 다양한 구현 방식이 존재하며, CHES에서는 저면적, 고성능의 다양한 설계방식이 제안되고 있다[39-41].

3.2. 고속화 구현 기법 연구 동향

암호 알고리즘이 현실의 산업에서 사용되기 위해서는 보안의 기밀성을 보장하면서 주어진 컴퓨팅 자원에 최적화되어 동작할 수 있어야 한다. 고속화 구현은 단순히 새로운 기교를 발명하여 알고리즘의 전반적인 성능을 향상하는 분야뿐만 아니라, 고사양 CPU에 내장된 SIMD(Single Instruction Multiple Data) 또는 그래픽 카드의 CUDA(Compute Unified Device Architecture) 등의 특수한 컴퓨팅 환경에서 최적화된 암호 구현에 관한 연구 역시 포함한다[42,43]. SIMD는 벡터 형태의 데이터를 병렬처리를 통해 연산을 수행함으로써 기본 연산에 비해 빠른 처리 효과를 가능하게 하며, 암호 알고리즘을 구현할 경우 블록 단위의 입력데이터를 Byte(8bit) 또는 Word(32bit) 이상의 단위로 처리할 수 있어 벡터 구성에 따라 다양한 고속화 구현이 가능하다. CUDA는 NVIDIA사에서 제공하는 범용 GPU 프로그래밍 라이브러리이다. GPU의 구조는 작은 프로세서의

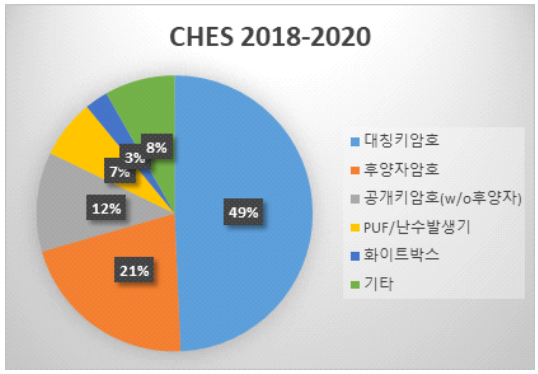
배열로 되어있기 때문에 병렬 연산에서 탁월한 성능을 보여주고 있고, 이러한 고성능의 병렬 연산은 암호 및 부채널 분야에서 다양한 적용이 가능하다. CHES에서는 암호 프리미티브 연산의 가속기와 관련된 연구가 주를 이루지만[44-46], 해시의 충돌 쌍을 찾는 전수조사 가속기와 같은 다른 관점의 고속화 구현 역시 논의되고 있다[47].

3.3. PUF/난수 발생기 연구 동향

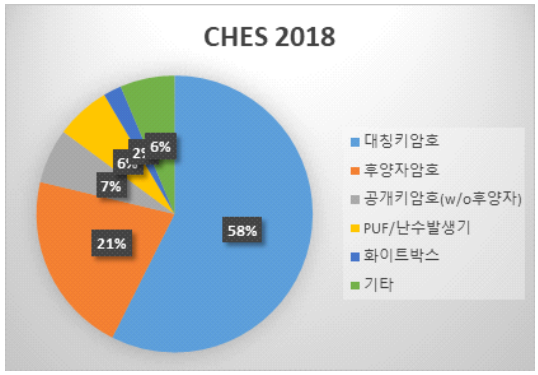
마치 인간의 지문이나 홍채와 같은 생체 정보처럼 각각의 기기의 고유의 특성인 PUF(Physically Unclonable Function)는 반도체 칩의 제조공정 특성에 따라 자연스럽게 나타나는 각 반도체 칩의 고유의 물리적인 특성이다. 즉, 아무리 똑같은 방법으로 기기를 만들어도 절대로 그 고유한 특성만큼은 복제할 수 없는 기술이다. 하드웨어 난수 발생기는 물리적 소스 데이터를 이용하여 난수를 생성하는 장치이다. 난수 발생기는 먼저 하드웨어의 잡음원을 수집하고 이를 디지털화 및 사후처리한 결과를 난수로 사용한다. 이때 PUF는 잡음원으로 사용될 가능성이 있고, 이러한 이유로 PUF와 난수 발생기는 서로 상보적인 연구가 주로 이루어진다[48]. CHES에서 PUF를 주목하는 이유는 고유의 독특한 특성을 이용하여 암호 알고리즘에 키 생성 알고리즘으로 사용할 수 있을 뿐만 아니라[49,50], 공격자 관점에서 PUF 정보를 복원 및 복제하여 난수 발생기를 통해 만들어지는 비밀키를 유추할 수 있는 등 다양한 부채널 취약점을 내포하고 있기 때문이다[51].

Ⅳ. 암호 알고리즘 종류별 연구 추의 분석

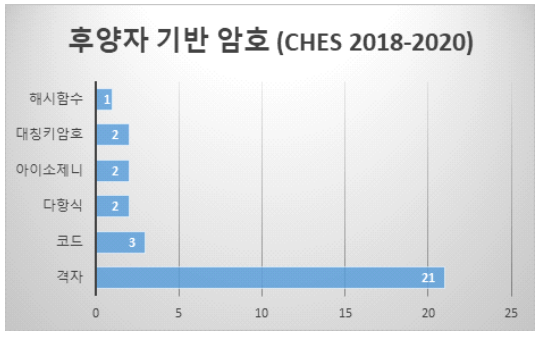
본 장에서는 최근 CHES에 발표된 부채널 공격, 대응기술, 구현의 대상이 되는 암호 알고리즘이 어떠한 방향으로 연구가 진행되는지 논의한다. [그림 11-15]와 [표 4]는 2018년도부터 3년 동안 CHES에서 발표된 논문 중 부채널 분야에 적용 대상이 되었던 암호 알고리즘 관련 논문의 편수이다. 대칭키 암호는 분석 및 적용의 편의성에 의하여 가장 다방면으로 부채널 분야에 연구 대상이 암호 알고리즘이다. 해당 절에서 추가로 설명하겠지만, 대칭키 암호는 단순히 AES와 같은 표준 블록 암호뿐만 아니라 부채널 대응기술 적용이 쉬운 암호 개발, ARX 블록 암호와 같은 경량암호, 비밀키를 자주 바꿔야 하는 환경을 위한 트윅커블(Tweakable) 블록 암호 및 암호 모드와 같은 다양한 종류의 대칭키 암호가 연구된다. 후양자 암호는 따로 관련 논문 편수를 측정해 볼 정도로 비중 있는 암호 알고리즘으로 부상하고 있다. 물론 RSA와 ECC로 대표되는 기존의 공개키 암호에 대하여 구현 및 머신러닝 기반 공격과 같은 신규 부채



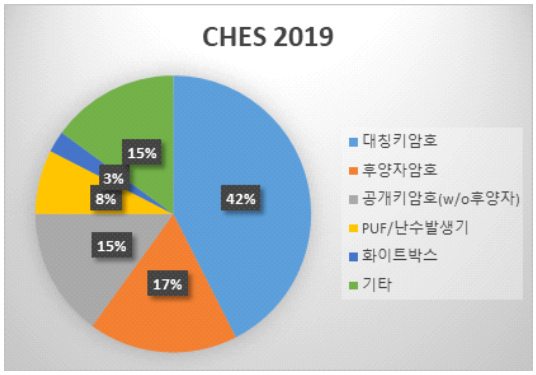
〔그림 11〕 부채널 분석 대상 알고리즘 (CHES 2018-2020)



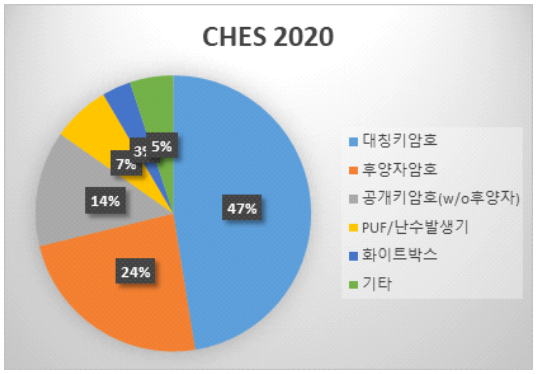
〔그림 12〕 부채널 분석 대상 알고리즘 (CHES 2018)



〔그림 13〕 부채널 분석 대상 후양자 알고리즘



〔그림 14〕 부채널 분석 대상 알고리즘 (CHES 2019)



〔그림 15〕 부채널 분석 대상 알고리즘 (CHES 2020)

〔표 4〕 최근 3년 CHES 발표 논문 (부채널 분석 대상 알고리즘)

종류	2018년도	2019년도	2020년도
대칭키 암호	27	17	28
후양자 암호	10	7	14
공개키 암호 (w/o 후양자)	3	6	8
PUF/난수 발생기	3	3	4
화이트 박스 암호	1	1	2
기타	3	6	3

널 분석 역시 꾸준히 제안되고 있다. 이 외에 PUF/난수 발생기, 화이트 박스 암호 등과 같은 다양한 암호 알고리즘에 관하여 부채널 연구가 진행되고 있다. 이후 절에서는 CHES에서 가장 비중 있게 연구 및 적용되는 대칭키, 공개키 및 후양자, 화이트박스 암호의 추이를 분석한다.

4.1. 대칭키 암호 알고리즘 추의 분석

대칭키 암호는 암호문을 생성할 때 사용하는 키와 암호문으로부터 평문을 복원할 때 사용하는 키가 같은 암호 시스템으로 해외 표준암호 AES, DES가 대표적이다. 가장 여러 방면에서 사용되는 암호 알고리즘인 만큼 CHES에서도 가장 공격 및 대응기술 연구의 주요 대상이 되고 있다[52]. AES와 같은 표준 블록 암호는 주로 신규 공격의 대상과 잘 알려진 대응기술 적용의 최적화 이슈로 다루어지고 있으며, 그 이외의 연구주제로 대칭키 암호 알고리즘은 컴퓨팅 자원이 부족한 IoT 환경에서 주로 사용되는 ARX 블록 암호와 같은 경량암호와[53], 트윅(Tweak)을 이용하여 같은 평문에 다른 암호문을 생성하도록 설계된 트윅커블 블록 암호 및 암호 모드 등이 있을 수 있다[54]. 이러한 시도는 블록 암호에 부채널 대응기술의 적용이 쉽도록 구조를 설계하는 데 목적이 있다. 특히 비선형 연산을 암호학적 안전성을 만족하면서, 그 구조가 부채널 대응기술 적용에 필요한 추가비용이 최소가 되도록 최대한 간결하게 설계하는 방안이 주요한 연구 초점이다.

4.2. 공개키 및 후양자 암호 알고리즘 추의 분석

사전에 비밀키를 나누어 가지지 않은 사용자들이 안전하게 통신할 수 있는 공개키 암호는 한 쌍의 키(공개키, 개인키)가 존재하며, 암호화에 사용되는 공개키는 누구나 알 수 있지만, 복호화에 사용되는 개인키는 키의 소유자만이 알 수 있어야 한다[55]. 대표적인 공개키 암호 RSA와 ECC는 각각 소인수분해와 이산대수 문제를 기반하여 설계된 암호 알고리즘이다. 그러나 양자 컴퓨터의 발전과 쇼어 알고리즘의 개발로 기존의 소인수분해와 이산대수 문제에 기반한 공개키 암호가 취약해짐에 따라 양자 컴퓨터에 내성이 있는 후양자 암호에 관한 관심이 증가하고 있다. 후양자 암호는 양자 컴퓨터를 이용한 공격에 다항 시간 내에 뚫리지 않으리라고 기대되는 암호이다. 후양자 암호는 기반하는 암호학적 문제에 따라 격자, 코드, 다항식, 해시함수, 대칭키 암호, 아이소제니 기반 암호로 분류될 수 있다. [그림 13]은 최근 3년 동안 CHES에서 발표된 후양자 암호 관련 논문을 정리한 그림이다. CHES에서 후양자 암호에 관한 연구는 초기 단계를 지나 성숙하는 과정 초반으로 분석되

는데, 이론적인 공격 및 대응기술을 제안하는 시기가 지나고 구체적인 고속화 구현 및 구현물에 대한 정밀한 공격이 발표되고 있다. 각각의 후양자 암호를 간략하게 살펴보면, 격자 기반 암호는 SVP (Shortest Vector Problem)인 좌표 안에 기본 벡터가 주어지면 이를 기반으로 하여 가장 짧은 벡터를 다항 시간 안에 찾기 어렵다는 문제와 CVP (Closest Vector Problem)인 좌표 안에 기본 벡터들이 주어졌을 때 이를 표현할 수 있는 가장 가까운 벡터를 찾기 어렵다는 문제에 기반한다. 논문 대부분은 격자 기반 후양자 암호에서 나오는데 다양한 후보 알고리즘에 대한 부채널 취약점 분석 및 대응기술 제안이 주를 이루고 있다[56,57]. 이 외의 후양자 암호는 적은 편수이긴 하나 꾸준히 취약점 보고 및 대응기술 개발이 이루어지고 있다. 코드 기반 암호는 선형 코드에 대한 디코딩이 어려움에 기반한 암호이며, 코드상에 에러를 포함해 실제 메시지를 도출시키는 것이 매우 어렵게 하는 기본 바탕에서 부채널 대응기술이 적용된 논문이 제안되었다[58]. 다항식 기반 암호는 매우 큰 행렬로 된 다항식의 해를 구하는 연산의 어려움을 이용하며, 아이소제니 기반 암호는 Supersingular elliptic curve 상에서의 연산 어려움에 기반하고, 해시 기반 암호는 해시함수의 특징인 충돌 저항성과 대칭키 기반 후양자 암호는 비밀키 크기를 늘림으로 양자 내성을 보장한다. 각각의 후양자 암호에 대해서도 부채널 공격과 [59,60], 고속화 구현의 대상으로 연구가 발표되었다 [61-64].

4.3. 화이트박스 알고리즘 추의

DRM(Digital rights management)은 출판자 또는 저작권자가 그들이 배포한 디지털 자료나 하드웨어의 사용을 제어하고 이를 의도한 용도로만 사용하도록 제한하는 데 사용되는 기술이다[65]. 디지털 정보의 불법 유출을 방지하기 위한 핵심 기술인 화이트 박스 암호는 암호 시스템의 사용자 역시 악의적인 공격자로 가정하고, 이러한 오픈된 환경에서조차 비밀키의 보안이 유지되도록 개발된 암호 알고리즘이다. 부채널 분야에서 화이트 박스 분석은 차분 계산 분석 (Differential computation analysis)이 주를 이룬다[66]. 차분 계산 분석은 소스 코드가 동작하는 과정에서 메모리를 읽거나 쓸 때 발생하는 바이너리 정보를 분석하여 비밀정보를 복원하는 공격이다. 최근 CHES에 발표되는 화이트 박스 암호 연구는 차분 계산 분석에 안전하도록 대응기술을 개발하고 제안된 대응기술에 취약점이 없는지의 피드백 과정을 반복하며 고도화 및 정밀화되어가고 있다[67-70].

Ⅴ. 결 론

CHES 보안 컨퍼런스는 암호 알고리즘의 하드웨어/소프트웨어 구현의 설계 및 분석에 대한 다양한 성과가 발표되는 대규모 복합연구 학회이다. 본 기고에서는 부채널 공격 관점, 부채널 대응기술과 부채널 분야에서 구현 이슈, 부채널 공격 및 대응기술 적용의 대상 암호 알고리즘의 최근 학회 동향을 분석해보았다. 이를 위하여 오류주입 공격, 머신러닝 기반 부채널 공격, 캐시공격, 부채널 누출 검증 방법론과 부채널 분야에서의 역공학에 관한 내용을 소개하고 최신 논문의 흐름에 대하여 논의하였다. 소프트웨어 고차 마스킹과 하드웨어 TI, PUF/난수 발생기 동향을 분석하였으며, 대칭키 및 공개키 암호를 비롯하여 화이트박스 암호와 관련된 논문을 살펴보았다. 이러한 CHES 컨퍼런스의 주제별 연구 동향 분석 결과는 부채널 분석 연구자에게 유용한 정보를 제공하고 향후 연구 방향에 대한 중요한 지표가 될 수 있을 것이다.

참 고 문 헌

[1] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. *Springer Science & Business Media*, 2008.

[2] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." *Annual International Cryptology Conference. Springer*, Berlin, Heidelberg, 1996.

[3] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." *Annual international cryptology conference. Springer*, Berlin, Heidelberg, 1999.

[4] Brier, Eric, Christophe Clavier, and Francis Olivier. "Correlation power analysis with a leak-

age model." *International workshop on cryptographic hardware and embedded systems*. Springer, Berlin, Heidelberg, 2004.

[5] Oswald, Elisabeth, et al. "A side-channel analysis resistant description of the AES S-box." *International workshop on fast software encryption*. Springer, Berlin, Heidelberg, 2005.

[6] Snouffer, Ray, Annabelle Lee, and Arch Oldenhoeft. *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2.* BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.

[7] Wouters, Lennert, et al. "Dismantling DST80-based Immobiliser Systems." *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.2 (2020): 99-127.

[8] Wouters, Lennert, et al. "Fast, furious and insecure: Passive keyless entry and start systems in modern supercars." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 66-85.

[9] Weissman, Zane, et al. "JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms." *arXiv preprint arXiv*:1912.11523 (2019).

[10] Krautter, Jonas, Dennis RE Gnad, and Mehdi B. Tahoori. "FPGAhammer: Remote voltage fault attacks on shared FPGAs, suitable for DFA on AES." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 44-68.

[11] Zhang, Fan, et al. "Persistent fault analysis on block ciphers." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 150-172.

[12] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." *nature* 521.7553 (2015): 436.

[13] Wu, Lichao, and Stjepan Picek. "Remove some noise: On pre-processing of side-channel measurements with autoencoders." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 389-415.

[14] Hoang, Anh-Tuan, Neil Hanley, and Maire O'Neill. "Plaintext: A Missing Feature for Enhancing the Power of Deep Learning in Side-Channel Analysis?." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 49-85.

[15] Carbone, Mathieu, et al. "Deep learning to evaluate secure RSA implementations." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 132-161.

[16] Timon, Benjamin. "Non-profiled deep learning-based side-channel attacks with sensitivity analysis." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 107-131.

[17] Robyns, Pieter, Peter Quax, and Wim Lamotte. "Improving cema using correlation optimization." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 1-24.

[18] Robyns, Pieter, Peter Quax, and Wim Lamotte. "Improving cema using correlation optimization." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 1-24.

[19] Kocher, Paul, et al. "Spectre attacks: Exploiting speculative execution." *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019.

[20] Yarom, Yuval, and Katrina Falkner. "FLUSH+ RELOAD: a high resolution, low noise, L3 cache side-channel attack." *23rd {USENIX} Security Symposium ({USENIX} Security 14).* 2014.

[21] Huo, Tianlin, et al. "Bluethunder: A 2-level directional predictor based side-channel attack against sgx." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 321-347.

[22] Dall, Fergus, et al. "Cachequote: Efficiently recovering long-term secrets of SGX EPID via cache attacks." (2018).

[23] Cooper, Jeremy, et al. "Test vector leakage assessment (TVLA] methodology in practice." *International Cryptographic Module Conference*. Vol. 20. 2013.

[24] Moradi, Amir, et al. "Leakage detection with the x2-test." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 209-237.

[25] Papachristodoulou, Louiza, et al. "Practical Evaluation of Protected Residue Number System Scalar Multiplication." (2019).

[26] de Chérisey, Eloi, et al. "Best Information is Most Successful." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 49-79.

[27] Du, Dongdong, et al. "Self-referencing: A scalable side-channel approach for hardware Trojan detection." *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, Berlin, Heidelberg, 2010.

[28] Albartus, Nils, et al. "DANA Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 309-336.

[29] Hoffmann, Max, and Christof Paar. "Stealthy Opaque Predicates in Hardware--Obfuscating Constant Expressions at Negligible Overhead." *arXiv preprint arXiv*:1910.00949 (2019).

[30] Blömer, Johannes, Jorge Guajardo, and Volker Krummel. "Provably secure masking of AES." *International workshop on selected areas in cryptography*. Springer, Berlin, Heidelberg, 2004.

[31] Sokolov, Danil, et al. "Design and analysis of dual-rail circuits for security applications." *IEEE Transactions on Computers* 54.4 (2005): 449-460.

[32] Rivain, Matthieu, and Emmanuel Prouff. "Provably secure higher-order masking of AES." *International Workshop on Cryptographic Hardware and Embedded Systems.* Springer, Berlin, Heidelberg, 2010.

[33] Coron, Jean-Sébastien, Franck Rondepierre, and Rina Zeitoun. "High order masking of look-up tables with common shares." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 40-72.

[34] Bettale, Luk, Jean-Sébastien Coron, and Rina Zeitoun. "Improved high-order conversion from Boolean to arithmetic masking." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 22-45.

[35] Oder, Tobias, et al. "Practical CCA2-secure and masked ring-LWE implementation." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 142-174.

[36] Wang, Weijia, et al. "Efficient and Private Computations with Code-Based Masking." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 128-171.

[37] Bache, Florian, et al. "High-Speed Masking for Polynomial Comparison in Lattice-based KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 483-507.

[38] Bilgin, Begül, et al. "A more efficient AES threshold implementation." *International Conference on Cryptology in Africa.* Springer, Cham, 2014.

[39] Moos, Thorben, et al. "Glitch-Resistant Masking Revisited." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 256-292.

[40] Sugawara, Takeshi. "3-share threshold implementation of AES S-box without fresh randomness." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 123-145.

[41] De Meyer, Lauren, Oscar Reparaz, and Begül Bilgin. "Multiplicative masking for AES in hardware." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 431-468.

[42] Rebeiro, Chester, David Selvakumar, and A. S. L. Devi. "Bitslice implementation of AES." *International Conference on Cryptology and Network Security*. Springer, Berlin, Heidelberg, 2006.

[43] Manavski, Svetlin A. "CUDA compatible GPU as an efficient hardware accelerator for AES

cryptography." *2007 IEEE International Conference on Signal Processing and Communications*. IEEE, 2007.

[44] Alkim, Erdem, et al. "Cortex-M4 Optimizations for {R, M\} LWE Schemes." *IACR Cryptol. ePrint Arch.* 2020 (2020): 12.

[45] Mera, Jose Maria Bermudo, Angshuman Karmakar, and Ingrid Verbauwhede. "Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 222-244.

[46] Al Badawi, Ahmad, et al. "High-performance FV somewhat homomorphic encryption on GPUs: An implementation using CUDA." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 70-95.

[47] Zhang, Zhendong, and Peng Liu. "A Hybrid-CPU-FPGA-based Solution to the Recovery of Sha256crypt-hashed Passwords." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 1-23.

[48] O'donnell, Charles W., G. Edward Suh, and Srinivas Devadas. "PUF-based random number generation." *In MIT CSAIL CSG Technical Memo 481* (2004).

[49] Ueno, Rei, Kohei Kazumori, and Naofumi Homma. "Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 86-128.

[50] Immler, Vincent, and Karthik Uppund. "New Insights to Key Derivation for Tamper-Evident Physical Unclonable Functions." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 30-65.

[51] Wisiol, Nils, et al. "Splitting the interpose PUF: A novel modeling attack strategy." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 97-120.

[52] Bhasin, Shivam, et al. "SITM: See-In-The-Middle Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 95-122.

[53] Adomnicai, Alexandre, Zakaria Najm, and Thomas Peyrin. "Fixslicing: A New GIFT Representation." *IACR Cryptol. ePrint Arch*. 2020 (2020): 412.

[54] Naito, Yusuke, and Takeshi Sugawara. "Lightweight authenticated encryption mode of operation for tweakable block ciphers." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 66-94.

[55] Forouzan, Behrouz A. Cryptography & network security. McGraw-Hill, Inc., 2007.

[56] Wang, Wen, et al. "Parameterized Hardware Accelerators for Lattice-Based Cryptography and Their Application to the HW/SW Co-Design of qTESLA." *IACR Cryptol. ePrint Arch.* 2020 (2020): 54.

[57] Ravi, Prasanna, et al. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 307-335.

[58] Wang, Weijia, et al. "Efficient and Private Computations with Code-Based Masking." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 128-171.

[59] Kannwischer, Matthias J., Peter Pessl, and Robert Primas. "Single-Trace Attacks on Keccak." *IACR Cryptol. ePrint Arch.* 2020 (2020): 371.

[60] Park, Aesun, et al. "Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 500-523.

[61] Massolino, P. M., et al. "A compact and scalable hardware/software co-design of sike." (2020).

[62] Faugère, Jean-Charles, Ludovic Perret, and Jocelyn Ryckeghem. "Software Toolkit for HFE-based Multivariate Schemes." 2019.

[63] Seo, Hwajeong, et al. "SIDH on ARM: faster modular multiplications for faster post-quantum supersingular isogeny key exchange." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 1-20.

[64] Kales, Daniel, and Greg Zaverucha. "Improving the Performance of the Picnic Signature Scheme." *IACR Cryptol. ePrint Arch.* 2020 (2020): 427.

[65] Chow, Stanley, et al. "White-box cryptography and an AES implementation." *International Workshop on Selected Areas in Cryptography.* Springer, Berlin, Heidelberg, 2002.

[66] Bos, Joppe W., et al. "Differential computation analysis: Hiding your white-box designs is not enough." *International Conference on Cryptographic Hardware and Embedded Systems.* Springer, Berlin, Heidelberg, 2016.

[67] Derbez, Patrick, et al. "On recovering affine encodings in white-box implementations." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 121-149.

[68] Rivain, Matthieu, and Junwei Wang. "Analysis and improvement of differential computation attacks against internally-encoded white-box implementations." *IACR Tran0sactions on Cryptographic Hardware and Embedded Systems* (2019): 225-255.

[69] Bock, Estuardo Alpirez, et al. "On the Security Goals of White-Box Cryptography." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 327-357.

[70] Goubin, Louis, Matthieu Rivain, and Junwei Wang. "Defeating State-of-the-Art White-Box Countermeasures with Advanced Gray-Box Attacks." *IACR Cryptol. ePrint Arch.* 2020 (2020): 413.

〈저 자 소 개〉

김 한 빛 (HanBit Kim)

정회원

2014년 2월 : 고려대학교 신소재공학 학사

2016년 2월 : 고려대학교 정보보호대학원 석사

2020년 8월 : 고려대학교 정보보호대학원 박사

2020년 9월~현재 : 고려대학교 정보보호대학원 연구원

<관심분야> 부채널 공격 및 대응기술, 암호 시스템 안전성 분석·평가 및 고속구현

김 희 석 (HeeSeok Kim)

종신회원

2006년 2월 : 연세대학교 수학과 학사

2008년 2월 : 고려대학교 정보보호대학원 석사

2011년 8월 : 고려대학교 정보보호대학원 박사

2011년 9월~2012년 12월 : Bristol University 박사후연구원

2013년 2월~2016년 8월 : 한국과학기술정보연구원(KISTI) 선임연구원

2015년 3월~2016년 8월 : 과학기술연합대학원대학교(UST) 조교수

2016년 9월~현재 : 고려대학교 과학기술대학 인공지능사이버보안학과 부교수

<관심분야> 부채널 공격, 암호 시스템 안전성 분석 및 고속구현, 암호 칩 설계 기술, 보안관제, 네트워크 보안