정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

CHES 2020을 중심으로 살펴본 SW/HW 암호 분석 및 구현 기술 연구 동향

안 상 우*, 송 진 교*, 박 보 선**, 서 석 충***

요 약

세계적으로 저명한 학회인 Cryptogrpahic Hardware and Embedded Systems(CHES)에서는 매년 부채널 공격, 암호 S/W, H/W 구현을 포함하는 정보 보안 분야에서의 화제가 되는 분야를 연구하고 공유한다. CHES 2020의 경우 부채널 공격, 양자 내성 암호, 머신 러닝과 같이 최근에 제시되어 활발하게 연구가 진행되고 있는 주제뿐만 아니라 역공학, 하드웨어 구현, 타원 곡선 암호, 화이트 박스 등의 다양한 결과들이 발표되었다. 본 논문에서는 CHES 2020을 통해 암호화 소프트웨어/하드웨어 및 임베디드 시스템에서의 보안 기술 개발 및 연구 동향을 살펴보며, 이에 따른 향후 연구 전망을 제시한다.

Ⅰ. 서 론

단순 데이터 암호화를 넘어서, 최근 정보 보안 분야에서의 다양한 기술들은 갈수록 확장되고 고도화되고 있다. 대표적으로는 양자 컴퓨터 개발로 인해 기존 공개키 암호를 위협할 수 있는 양자 알고리즘에 대응하기 위한 양자 내성 암호(Post-Quantum Cryptography, PQC)가 개발되거나, 부채널 공격(Side-Channel Attack, SCA)을 통해 물리적인 누수 정보를 수집 및 분석하여 암호 알고리즘을 공격하는 방법들이 제시되거나, 동형 암호(Homomorphic Encryption)나 검색 가능한 암호(Searchable Encryption) 등 고도화된 암호 기법들이 개발되고 있다.

매년 새로운 위험성이 제시되고, 새로운 보안 기술이 개발되고 연구됨에 따라, 이러한 정보를 공유하고 근미래 기술의 방향성을 논의할 수 있는 자리인 학회의 중요성이 증가하고 있다. 대표적으로는 매년 암호학적인 소프트웨어/하드웨어 구현에 대한 설계 및 분석의 최신 결과가 발표되는 국제 학회인 CHES(The annual Conference on Cryptographic Hardware and Embedded Systems)가 있다.

2020년 9월에 진행된 CHES 2020에서는 총 12개의 세션에서 키 노트 세션을 포함한 총 62개의 주제에 대한 온라인 컨퍼런스가 진행되었다. 12개의 세션을 큰 분야로 묶으면 새로운 암호 설계 기법(New Designs), 역공학(Reverse Engineering), 부채널 공격, 타원곡선 및 아이소제니 기반 구현(ECC and Isogenies), 물리적 복사방지기술 및 화이트 박스 기법(PUFs and White-Box Cryptography), 하드웨어 환경에서의 최적화 구현(Hardware Implementation), 머신 러닝(Machine Learning), 격자 기반 암호(Lattice-Based Cryptography)로 총 8개의 분야로 정리할 수 있다.

본 논문에서는 이러한 CHES 2020에 발표된 최신 연구 결과를 포함하고 있는 논문들에 대해 분야별로 정리하고 분석한다. 분야별로 절을 구성하여 2장에서는 CHES 2020의 각 분야에 대한 연구 및 개발 동향을 소개하고, 3장에서는 결론 및 향후 연구 전망을 제시한다.

Ⅱ. CHES 2020 기술 개발 및 연구 동향

2.1. CHES 2020 경향 분석

본 절에서는 CHES 2020에 발표된 논문들에 대한 연구 경향을 분석한다. CHES 2020에는 총 60편의 논

이 논문은 2020년도 정부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2019R1F1A1068494)
* 국민대학교 금융정보보안학과(pinksnail06@kookmin.ac.kr, sjk9304@kookmin.ac.kr)
** 국민대학교 정보보안암호수학과(20175206@kookmin.ac.kr)
*** (교신 저자) 국민대학교 정보보안암호수학과 (scseo@kookmin.ac.kr)

〔표 1〕 CHES 2020 국가별 등재 논문 수

국가	논문 수
독일	9
벨기에	8
미국	7
네덜란드	5
중국	5
프랑스	5
싱가포르	4
영국	4
핀란드	3
이탈리아	2
인도	2
일본	2
대만	1
오스트리아	1
체코	1
터키	1
총 계	60

문이 소개되었으며 12개의 세션으로 분류되었다. 국가별 논문 등재 수는 표 1에 내림차순으로 정리되어 있다. 새로운 암호 설계 기법 세션에서는 총 4편의 논문이 소개되었으며, 역공학 세션에서는 3편, 대칭키 암호 알고리즘에 대한 부채널 공격 세션에는 6편, 타원 곡선 암호와 아이소제니 기반 암호 세션에는 5편, 부채널 공격 이론 및 평가(SCA Theory and Evaluation) 세션에는 6편, 수정 방지 기술 및 화이트 박스 암호 세션에는 4편, 하드웨어 환경에서의 최적화 구현 세션에는 4편, 머신 러닝 세션에는 6편, 격자 기반 암호 세션에는 6편, 부채널 공격 대응 기법(SCA Countermeasures) 세션에는 6편, 공개키 암호에 대한 부채널 공격(SCA of Public-Key Schemes) 세션에는 6편, 그리고 오류 주입 공격(Faults) 세션에는 4편의 논문이 소개되었다. 분야별 논문 수는 표 2에서 확인할 수 있다. 12개 세션을 키워드 별로 크게 분류하면 부채널 공격, 하드웨어 구현, 격자 기반 암호, 타원 곡선 암호, 화이트 박스로 나눌 수 있다. CHES 2020에 소개된 논문들의 대표 경향은 총 34편의 논문이 포함된 부채널 공격 분야로 집계되었다.

2.2. 부채널 공격 연구 동향

기존의 수학적인 논리에 의해 암호 알고리즘을 공격할 수 있는 선형 공격(Linear Cryptanalysis)이나 차분 공격(Differential Cryptanalysis)과는 다르게 암호가 실제로 동작하는 디바이스에서 발생하는 전력 소모량, 전자기파 등과 같은 다양한 누수 정보를 이용하여 암호키를 찾아내는 공격 기법을 부채널 공격이라고 하며, 이러한 부채널 공격 기법이 제안됨에 따라 암호 알고리즘을 구현할 때 부채널 공격 관점에서의 안전성을 추가적으로 고려하게 되었다.

부채널 공격은 크게 비침투 공격(Non-Invasive Attack)과 침투 공격(Invasive Attack)으로 나눌 수 있다. 대표적인 비침투형 공격 유형의 부채널 공격 방법은 단순 전력 분석(Simple Power Analysis, SPA), 차분 전력 분석(Differential Power Analysis, DPA), 그리고 상관관계 전력 분석(Correlation Power Analysis, CPA) 등이 있다[1]. 이러한 공격은 대부분 암호 알고리즘이 탑재된 디바이스가 동작하면서 발생하는 전력/전자파를 분석하여 특정 알고리즘에서의 연산을 구분하거나 특정 입력값을 알아낼 수 있다. 침투 공격의 대표적인 공격은 오류 주입 공격(Fault Attack)이 있다. 디바이스에 주로 가하는 오류 주입 방법은 디바이스에 가하는 전압을 급격하게 변화시키거나 레이저 오류 주입 방식, 강한 EM 방사를 통한 오류 주입 방식 등이 있다. 이외에도 연산 시간의 차이를 분석하여 공격하는

〔표 2〕 CHES 2020 분야별 등재 논문 수

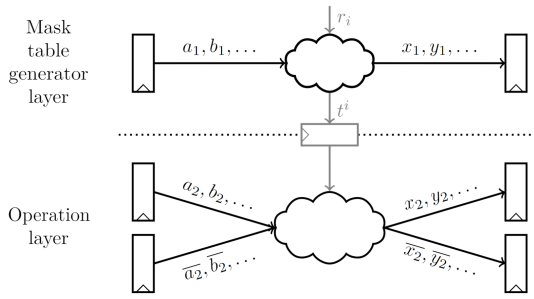
분야	논문 수
새로운 암호 설계 기법	4
역공학	3
대칭키 암호 알고리즘에 대한 부채널 공격	6
타원 곡선 암호와 아이소제니 기반 암호	5
부채널 공격 이론 및 평가	6
수정 방지 기술 및 화이트 박스 암호	4
하드웨어 환경에서의 최적화 구현	4
머신 러닝	6
격자 기반 암호	6
부채널 공격 대응 기법	6
공개키 암호에 대한 부채널 공격	6
오류 주입 공격	4
총 계	60

소요 시간 분석 공격(Timing Attack) 또한 부채널 공격의 일종으로 간주한다.

CHES 2020에서는 부채널 공격에 대한 연구가 가장 많이 발표되었다. CHES 2020에 공개된 부채널 공격에 대한 키워드를 크게 세 가지로 분류하면 다음과 같다: 대칭키 암호 알고리즘에 대한 부채널 공격, 진보된 부채널 공격 기법 구현, 그리고 부채널 공격 대응 기법 연구.

제시된 다양한 부채널 공격 가능성에 대한 연구 중에서는 다양한 대칭키 암호 알고리즘이 사용하는 구조인 SPN(Substitution Permutation Network)에 대한 차분 공격에 부채널 공격을 적용한 See-In-The-Middle 공격이 제안되었다[2]. 부채널 공격이 주로 수행되는 첫 번째나 마지막 라운드가 아닌, 중간 라운드에 대한 공격을 진행함으로써 AES, SKINNY, PRESENT 알고리즘에 대한 부채널 공격 분석 결과를 제시하였다. 또한 양자내성 암호를 포함한 다양한 암호 알고리즘에서 사용하고 있는 해시 함수인 SHA-3 알고리즘 Keccak에 대한 단일 파형 부채널 공격 방법이 제안되었다[3]. 공격 대상 알고리즘인 Keccak에 대한 성공률과 계산 시간 측면에서의 높은 공격 성능을 성취하기 위해 모델링과 메시지 전달 알고리즘에 대한 최적화된 부채널 공격 기법을 제안하였으며, SASCA(Soft-Analytical Side Channel Attacks)을 주 공격 기법으로 사용하여 Keccak에 대한 유의미한 분석 결과를 제시하였다. 이 이외에도 의사난수 생성기의 일종인 CTR_DRBG에 대한 256개 파형 내의 부채널 공격 기법[4]과 SPN 구조의 블록 암호 알고리즘인 Pilsung에 대한 일반적인 노트북으로도 8분 만에 성공시킬 수 있는 캐시 기반 부채널 공격을 진행한 연구가 소개되었다[5].

CHES 2020에는 부채널 공격에 대한 가능성을 연구한 분야 이외에도 부채널 공격에 대한 다양한 대응 기술을 개발한 연구도 다수 소개되었다. 그 중에서는 1차 부채널 공격 대응기법을 공격하는 2차 부채널 공격에 대한 추가적인 대응을 위한 마스킹(Masked)된 참조 테이블을 구성할 수 있는 방법이 제시되었다[6]. 해당 논문에서는 AES에 대하여 2차 마스킹 Sbox를 Vadnala's scheme을 응용하여 59바이트 크기로 무작위 테이블 압축 방식을 사용하여 AES를 마스킹하는 기술을 제안하였다. 그뿐만 아니라, CHES 2014에서 제안된 LUT-based maksed Dual-Rail with Pre-charge Logic(LMDPL) 기술을 활용하여 알고리즘의 지연 시간을 늘리지 않는 하드웨어에 대한 저전력 AES 마스킹 구현 기법이 제안되었다[7]. LMDPL에 대한 간단한 구조는 그림 1과 같다.

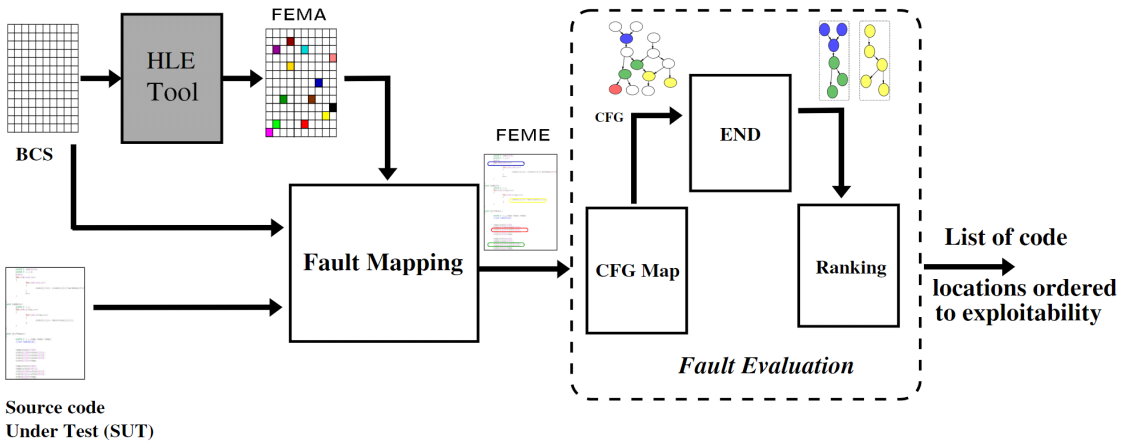


〔그림 1〕 LMDPL 모식도. 선형 가젯과 비선형 가젯이 Dual-rail로 동작한다. 각각의 LMDPL 가젯은 두 개의 공유된 불 마스킹 변수를 사용한다[6].

마스킹은 전력 분석을 방어하기 위하여 메시지나 키 값에 마스크 값을 반영하여 전력 소모량과 같은 누수 정보를 변경시키는 기법이다. 이러한 마스킹 기법 이외에도 알고리즘의 연산 방식을 메시지 또는 바이트 단위에서 비트 단위 또는 데이터가 나누어진(Slicing) 형태로 병렬 진행하여 누수 정보를 사용할 수 없게 변형시키는 효율적인 기술이 제안되었다[8]. 부채널 공격 중 오류 주입 공격 또한 소개되었는데, 그 중에서 블록 암호의 소프트웨어 구현을 위한 포괄적인 오류 주입 공격 취약성을 탐지하는 기술인 FEDS가 제안되었다[9]. FEDS의 모식도는 그림 2와 같다. 해당 논문에서는 컴파일러 기법과 모델 점검 기술을 결합한 프레임워크를 제안하여 사용함으로써 광범위한 오류 주입 공격의 취약성에 대한 종합적인 평가를 알고리즘 단계에서 수행할 수 있음을 제안하였다. 이러한 프레임워크를 사용해서 비트 슬라이싱(Bitslicing) 기법을 포함한 7종의 서로 다른 AES 구현물과 CLEFIA, CAMELLIA 구현물에 대한 프레임워크가 정상적으로 오류 주입 취약성에 대한 평가를 진행해 보였음을 증명하였다.

2.3. 하드웨어 최적화 구현 연구 동향

입력에 대한 출력값을 계산하도록 구현된 함수인 소프트웨어와는 달리 물리적 회로로 구성된 하드웨어는 구현 관점에서 소프트웨어와는 다른 양상을 보여준다. 최적의 연산을 진행할 수 있도록 설정된 하드웨어는 비슷한 환경에서의 소프트웨어의 작업 속도보다 향상된



〔그림 2〕 소프트웨어 구현의 활용 가능성을 탐지하는 FEDS 프레임워크 개요. HLE(High-Level Evaluation) 도구는 블록 암호로부터 알고리즘에 대한 오류 주입 공격 가능성에 대한 맵핑을 출력한다[8].

성능을 보여준다. 예를 들어, GPU에서의 부동 소수점 연산은 특정 연산을 다중 병렬 방식으로 수행하도록 설계되었으며, CPU 대비 향상된 다중 병렬 작업 수행 속도를 보여준다. 하지만, 하드웨어 구현은 소프트웨어 구현 대비 시간이 오래 소요되고 매번 새로운 회로를 만들기가 매우 힘들다. 이에 따라 내부에 수많은 논리 게이트를 탑재한 FPGA(Field Programmable Gate Arrays)를 사용하여 VHDL과 같은 언어로 소프트웨어 함수와 비슷한 동작을 취하는 회로를 구성할 수 있다는 장점을 활용한 다양한 연구가 수행되었다.

CHES 2020에서는 FPGA 환경을 대상으로 효율적인 하드웨어 구현 기술이 제안되었다. 이 중 SHA256crypt로 해싱된 암호에 대한 복구를 진행하기 위한 CPU-FPGA 기반 구현 기법이 제시되었다[10]. 기존 SHA256crypt와 같은 키 유도 함수(Key Derivation Function, KDF)의 단점을 하이브리드 장치인 CPU-FPGA를 활용하여 개선할 수 있는 방법이 제시되었다. 이에 따라 SHA256crypt로 해싱된 데이터에 대한 암호 복구를 위해 CPU는 비통합 실행 경로에 존재하는 암호 생성 및 계산 작업을 수행하고 FPGA는 통합 실행 경로에 존재하는 병렬 파이프라이닝(Pipelining)이 가능한 연산을 전담하여 처리하도록 구현되었다. 가속기를 활용한 효율적인 CPU-FPGA 하이브리드 기술은 그룹 스케줄링, 데이터 경로 정리 및 공간-시간 다중화와 같은 다양한 기술을 적용하여 추가적인 성능을 향상시키고 하드웨어 자원 부담을 줄일 수 있게끔 설계되었다.

효율적인 하드웨어 구현 이외에도 가상화된 FPGA 환경에서의 부채널 공격 등의 공격방법으로 인한 위험성을 증명하고 제시한 연구가 진행되었다[11]. 연구에 따르면 FPGA를 활용하여 인공 지능(Artificial Intelligence, AI) 및 기계 학습(Machine Learning) 영역에서 범용적인 하드웨어 가속기로서 모든 주요 클라우드 컴퓨팅 서버의 주요 구성 요소가 되었지만, FPGA 효율 극대화를 위해 사용되는 가상화 FPGA 기술은 잠재적인 보안 위험성이 존재함을 제기하였다. 일반적으로 부채널 공격은 광범위한 측정 장비를 갖춘 로컬 공격자에 의해 수행되었지만, FPGA 칩에서 논리적으로 격리된 설계 간에 오류 주입 공격 및 부채널 공격을 수행할 수 있었음을 밝혔다. 이러한 근거는 논리적으로 격리되었음에도 FPGA 칩의 모든 설계 구성 요소가 Power Distribution Network(PDN)을 통해 연결되어 있어서 가능해짐을 설명한다. 이러한 공격 방법을 통해 공격자는 FPGA의 서로 다른 영역에 여러 센서를 배치하여 지역화된 정보를 획득할 수 있다는 위험성을 제시하였다.

2.4. 머신 러닝을 활용한 암호기술 연구 동향

전통적인 컴퓨터 프로그램은 정해진 입력만을 받아 정해진 출력을 나오게 하는, 즉 규칙이 정해진 함수였다. 하지만 컴퓨터를 인간처럼 학습시켜 스스로 규칙을 만들어 결정할 수 있을 필요성이 대두되었으며, 이에 따라 인공 지능부터 딥 러닝(Deep Learning)까지의 다양한 연구 및 개발이 수행되었다.

머신 러닝의 목표는 특정 작업에 대하여 꾸준한 경험(Data)을 통하여 성능(Accuracy)를 높이는 것이다. 따라서 꾸준한 경험에 해당하는 좋은 품질의 학습 데이터는 기계학습에서 매우 중요한 요소로 여겨지며, 머신 러닝의 학습 요소를 지도 여부에 따라 크게 두 가지로 나눌 수 있다. 지도 학습(Supervised Learning)은 사람이 각각의 입력에 대하여 직접 개입해 레이블을 달아 컴퓨터에게 주면 컴퓨터가 입력과 레이블의 쌍으로 학습하는 방식이다. 지도 학습은 정확도가 높은 데이터를 사용할 수 있다는 장점이 있지만, 사람이 직접 입력에 대한 레이블을 달아야 하기 때문에 구할 수 있는 데이터양의 한계가 존재한다. 비지도 학습(Unsupervised Learning)은 컴퓨터가 스스로 입력만을 사용하여 학습하는 방식이다. 비지도 학습은 레이블이 없으므로 컴퓨터가 입력 데이터를 통계적으로 분류하고 분석하게 된다. 최근에는 현재의 상태(State)에서 최적의 행동(Action)을 최대의 보상(Reward)을 받을 수 있는 근거에 기초로 학습할 수 있게 만들어진 강화 학습(Reinforcement Learning)이 연구되고 있다.

딥 러닝은 머신 러닝의 특정 분야로, 연속된 층(Layer)을 겹겹이 쌓아 올려 구성한 신경망(Neural Network)이라는 모델을 사용하여 학습을 진행한다. 입력 데이터는 심층 신경망을 통과하면서 연속된 필터를 거쳐 올바른 출력에 대한 가중치를 가지게 된다. 딥 러닝은 이러한 과정에서의 정확성을 높이고, 올바른 답과 예측값의 차이(Loss)를 줄일 수 있도록 학습하는 것이 목표가 된다.

이러한 머신 러닝 기술은 다양한 분야에서 활용 및 연구되고 있으며, CHES 2020에서도 머신 러닝을 활용한 다양한 부채널 공격 분야의 연구를 소개하고 있다. 부채널 공격을 수행하기 위해선 전력 소모량 등의 누수 정보가 기록된 파형이 필요하다. 이러한 파형은 그림 정보로 여겨질 수 있으며, 그림 정보에 대한 학습에 특화된 머신 러닝의 CNN(Convolutional Neural Network) 방식을 사용하여 기존보다 적은 수의 파형으로도 컴퓨터를 학습시켜 올바른 비밀키 값을 찾거나, 수집된 파형 등에서의 잡음(Noise)를 줄일 수 있는 기법에 활용될 수 있다. CNN 방식을 적용하여 기존보다 25배 효율적인 Profiling Attack을 성공시킬 수 있는 방법이 제시되었으며[12], 부채널 공격 대응 기법이 적용되어 있는 암호 알고리즘에 대하여 딥 러닝을 사용하여 대응 기법이 적용되지 않은 일반 알고리즘을 찾을 수 있는 기법이 제안되었다[13]. 이 이외에도 딥 러닝을 활용하여 기존 부채널 공격 환경보다 악조건에 있는 데이터들을 보정하거나 더 적은 복잡도로 효율적인 부채널 공격을 수행할 수 있는 모델링을 제시한 연구가 다수 소개되었다[14].

2.5. 격자 기반 암호 연구 동향

양자 컴퓨팅(Quantum Computing) 시대가 도래하면서, Shor가 제시한 양자 알고리즘으로 인하여 RSA(Rivest-Shamir-Adleman)나 타원 곡선 암호(Elliptic Curve Cryptography, ECC) 같은 소인수 분해와 이산 대수의 어려운 문제를 기반으로 짜여진 알고리즘에 대한 위험성이 제기되었다. 근미래의 양자 알고리즘에 의한 잠재적인 위험성에 대비하기 위해 다양한 양자 내성 암호가 개발되었으며, NIST에서는 양자 내성 암호 표준화 산업을 통해 현재 라운드 3에서 양자 내성 암호로 지정될 알고리즘들을 심사하고 있다. NIST 양자 내성 암호 표준화 산업에서 경쟁하고 있는 알고리즘은 다양한 기반에서 개발이 되었으며, 격자(Lattice) 기반, 코드(Code) 기반, 다변수(Multi-Variable) 기반, 아이소제니(Isogeny) 기반, 해시(Hash) 기반으로 분류될 수 있다.

이 중에서도 가장 비중을 크게 차지하고 있는 기반은 격자 기반으로, 다양한 응용 환경을 지원하면서도 빠른 속도로 구현할 수 있다는 장점이 있다. 현재 NIST 양자 내성 암호 표준화 산업 라운드 3의 Finalist로 선정된 키 캡슐화 알고리즘(Key Encapsulation Mechanism, KEM)은 총 4개인데, 이 중 코드 기반인 McEliece를 제외한 나머지 CRYSTALS-KYBER, NTRU, SABER은 모두 격자 기반 암호 알고리즘이다.

CHES 2020의 격자 기반 암호 세션 중에서는 RLWR(Ring Learning With Rounding) 기반 격자 기반 암호 알고리즘인 SABER에서의 효율적인 곱셈 알고리즘을 위해 곱셈 연산을 수행하는 Toom-Cook 알고리즘에 대하여 lazy 보간법과 사전 연산 방법이 제안되었다[15]. 제안된 구현 기법에서는 256차 다항식 곱셈에서 3번의 다항식 곱셈마다 한 번씩 보간법을 적용하여 효율적으로 Toom-Cook 알고리즘에서의 보간 횟수를 줄였으며, 사전 연산 방법을 통하여 고정되는 입력값에

〔표 3〕 AVX2 환경에서 SABER의 최적화 구현 성능 향상치(cycles)

파라미터	기존 구현	최적화 구현	성능 향상치
l = 2	10199	7214	29.3%
l = 3	21356	13574	36.4%
l = 4	39039	24767	36.6%

대한 출력값을 사전 계산하여 Toom-Cook 알고리즘의 연산과정을 효율적으로 감소시킬 수 있는 방법이 포함되어 있다. 이러한 최적화 구현 결과, SABER에 최적화된 Toom-Cook 알고리즘을 사용하여 ARM Cortex-M4 환경에서 곱셈 연산의 수행 속도가 최대 37% 향상되었음을 제시하였으며, 또한, 메모리 사용량을 최대 5.7KB 줄일 수 있었음을 소개하였다. 논문에서 제시한 AVX2 최적화 구현 상에서의 곱셈 성능 향상치는 표 3과 같다.

LWE(Learning With Error) 격자 기반 암호 알고리즘에서는 효율적인 곱셈 연산을 위해서 NTT(Number Theoretic Transform)을 사용한다. 기존 NTT 대비 효율적인 모듈러 감산과 작은 차수의 다항식 곱셈을 처리하는 최적화된 NTT를 활용하여 LWE 격자 기반 암호 알고리즘인 NewHope과 MLWE(Modulo Learning With Error) 격자 기반 암호 알고리즘인 CRYSTALS-KYBER에 대한 최적화 기법이 제안되었다[16]. 이러한 ARM 환경 상에서의 최적화 구현 이외에도 하드웨어와 FPGA 환경에서의 격자 기반 암호 고속화 기술[17]과 RISC-V에서의 가속기[18]가 소개되었다.

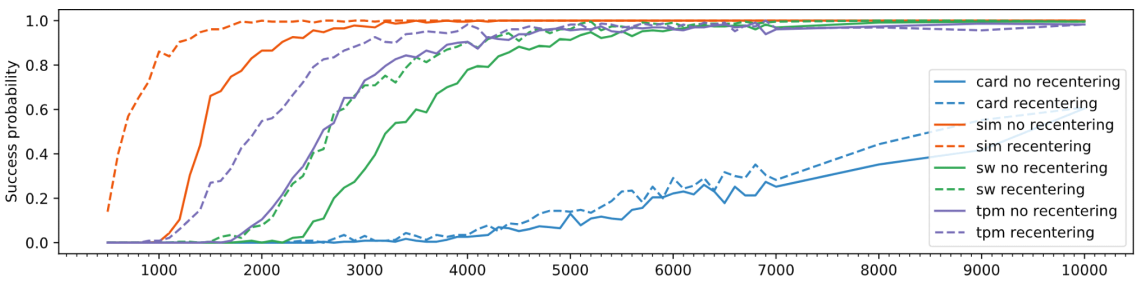
2.6. 타원 곡선 암호 연구 동향

타원 곡선 암호는 타원곡선을 기반으로 한 공개키 암호 방식으로, 기존 RSA 대비 키 길이가 짧다는 장점이 있다. 타원 곡선 암호는 유한체 상에서의 타원 곡선에 대한 효율적인 연산을 수행하며, 다양한 파라미터에 따라 타원 곡선을 선택할 수 있다는 장점이 있다. 이러한 장점으로 인해 키 교환(Elliptic Curve Diffie-Hellman, ECDH)이나 전자 서명(Elliptic Curve Digital Signature Algorithm, ECDSA)에 적극적으로 활용되고 있다.

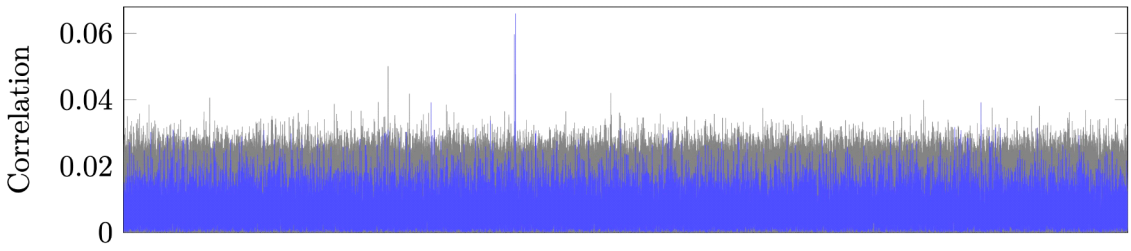
타원 곡선 암호는 현재 NIST를 중심으로 권장하는 파라미터인 Weierstrass Curve가 사용되고 있으며, 특정 환경에서의 보다 더 효율적인 연산을 위해 Edward Curve나 Montgomery Curve 등이 연구되고 있다. 또한, 타원 곡선이 표현되는 좌표계의 특성을 활용한 최적화 구현 기법 등이 연구되고 있으며 부채널 공격의 대상이 되는 타원 곡선 암호에 대한 안전성 분석 연구도 활발하게 수행되고 있다.

CHES 2020에 제안된 타원 곡선 암호 분야에서는 크게 안전성 분석 관점과 최적화 관점에서 주제를 분류할 수 있다. 최적화 관점에서는 짧은 Weierstrass Curve에 대한 타원 곡선 암호 기반 곱셈 방식인 Montgomery Ladders의 연산 부하를 줄이기 위하여 기존의 8M+4S+8A+1H (M:곱셈, S:제곱, A:덧셈, H:나눗셈) 연산보다 효율적인 8M+3S+7A 연산 수를 가지는 타원 곡선 암호 기반 곱셈 방식을 제안한다[19].

CHES 2020에서 Best Paper로 선정된 논문은 타원 곡선 암호 세션에서 소개되었는데, ECDSA 누설 잡음에 대한 격자 공격을 분석하는 주제를 제시한다[20]. 해당 연구에서는 자주 사용되는 Atmel AT90SC FIPS 140-2 인증 스마트카드 칩과 5개의 암호화 라이브러리(libgcrypt, wolfSSL, MatrixSSL, SunEC/OpenJDK, Crypto++)에서 ECDSA 인증 알고리즘 구현물에 대한 부채널 공격 취약점을 제시하고, 키를 복구하기 위해



〔그림 3〕 ECDSA 인증 알고리즘 구현물에 대한 recentering과 geometric bounds 기술을 사용한 SVP(Shortest Vector Problem) 기반 부채널 공격의 성공률[19].



〔그림 4〕 고차 차분 계산 공격 기술을 사용하여 화이트 박스가 적용된 알고리즘에 부채널 공격을 수행한 결과. 타겟은 3번째 Sbox의 첫 번째 비트를 잡았으며 올바른 추측키 후보가 다른 키 후보에 비해 명확하게 표시되는 것을 확인할 수 있다. 이 공격은 767개의 파형을 사용하며, 16 바이트 키 값 중 7 바이트를 복원할 수 있다〔21〕.

500개만의 서명 데이터를 요구하는 효율적이고 새로운 두 가지 방법을 제안한다. 이러한 방법을 실제 취약점에 적용하여 작성된 벤치마크에서는 이전에 발표된 모든 방법보다 TPM-FAIL 집합에 대한 성공적인 공격을 위해 훨씬 더 적은 수의 서명 데이터만을 필요로 함을 제시하였다. 해당 공격에 대한 ECDSA 인증 알고리즘 구현물에 대한 성공률은 그림 3에서 확인할 수 있다. 이뿐만 아니라, 소프트웨어 암호 라이브러리와 스마트 카드에 탑재된 타원 곡선 암호 구현물의 광범위한 분석을 위한 오픈 소스 툴을 공개하였다.

2.7. 화이트 박스 연구 동향

화이트 박스 암호(White-box Cryptography)는 공격자가 암호화 키를 쉽게 유추할 수 없도록 암호화 키 정보를 알고리즘에 내부에 포함시키는 기법이다. 기존 블랙 박스 암호에서는 디바이스의 물리적 차원에서의 정보 유출 위험성이 존재했지만, 화이트 박스 암호 기술을 통해 소프트웨어만으로 암호 알고리즘의 중간값 및 키 값을 보호하기 위한 다양한 기술 개발 및 연구가 수행되었다.

CHES 2020에서는 화이트 박스 암호화에 대한 기존 및 새로운 보안 개념에 대하여 논의가 되었으며, 화이트 박스 암호화의 일반적인 사용 사례인 디지털 권한 관리 및 모바일 결제 어플리케이션에 대한 적합성을 논평하는 연구 주제가 소개되었다[21]. 해당 주제에서는 화이트 박스에서의 새로운 보안 개념인 하드웨어 바인딩(IND-WHW)이 있는 화이트 박스 암호화의 중요성을 설명하고 그것을 공식적인 보안 개념으로 정의할 때 직면하는 문제들을 설명한다. 해당 연구에서는 화이트 박스 암호화에 대한 기존의 보안 개념의 한계를 제시하고, 하드웨어 바인딩을 이용한 모델 사이에서의 차이점을 제시한다.

이와 달리 화이트 박스 기술이 적용된 암호를 공격하는 방법이 제안된 연구 또한 CHES 2020에 소개되었는데[22], 해당 연구에서는 발전된 그레이 박스 공격(Gray-box Attack)을 이용하여 최신 화이트 박스 기술이 적용된 AES-128에 대한 성공적인 공격 기법을 제시하였다. 해당 연구에서는 선형/비선형 마스킹 및 셔플링(shuffling) 기법이 비트슬라이싱된 화이트 박스 구현물에 적용된 최신 화이트 박스 암호 구현물에 대한 공격을 소개한다. 공격 방법은 발전된 그레이 박스 공격으로 칭해지며, 고차 디코딩 공격(Higher-degree Decoding Analysis) 기술과 고차 차분 계산 공격(High-order Differential Computation Analysis) 기술을 포함한다. 그림 4는 고차 차분 계산 공격을 통해 측정한 파형 상관 계수의 그래프를 보여준다. 해당 공격 방법을 통한 파형과 시간 복잡도를 제시하며, 이뿐만 아니라 새로운 데이터 의존형 그레이 박스 공격 기법을 적용한 공격 시나리오를 소개한다. 이러한 공격 기법을 통해서 기존의 마스킹 기법을 깨뜨릴 수 있음을 소개하였다.

Ⅲ. 결 론

정보 기술의 발전에 따라 정보 보안의 중요성 또한 해가 거듭할수록 증가하고 있다. 다양한 정보 보안 기술의 발전으로 인하여 기존의 안전성이 위협될 수 있으며, 기존 보안 체제에 대한 잠재적인 위험성을 방지하기 위하여 새로운 기술들이 지속적으로 연구되고 있다. 전 세계에서 수행되고 있는 연구들의 진행 상황 및 동향 정보를 공유하고 협력할 수 있는 자리인 학회는 정보 보안 분야에서도 매우 중요한 위치에 속해 있다. 암호화

및 임베디드 시스템 분야에서의 대표적인 국제 학회인 CHES에서는 매년 부채널 공격, S/W 및 H/W 구현과 같은 정보 보안 분야에서 수행되고 있는 연구를 발표한다.

본 논문에서는 CHES 2020에서 제시된 다양한 연구 및 개발 동향을 소개한다. CHES 2020의 주 관심 분야는 부채널 공격, 격자 기반 암호, 머신 러닝이며, 이 이외에도 하드웨어 구현, 화이트 박스 등 다양한 연구가 진행되었다. CHES 2020에서는 부채널 공격 분야에서의 논문이 가장 많았으며, 대칭키 및 공개키 암호 알고리즘에 대한 부채널 공격, 오류 주입 공격, 머신 러닝을 활용한 부채널 공격, 부채널 대응 기법 등 다양한 부채널 공격에 대한 연구가 진행되고 있음을 분석하였다. 이러한 분석 결과를 통해 향후 정보 보안 분야에서의 주 연구 주제는 부채널 공격에 대한 새로운 공격 기술, 효율적인 공격 기술과 그에 대한 대응 기법이 적극적으로 연구될 것임을 확인할 수 있다.

CHES 2020에서의 연구 동향을 살펴봄으로써 정보 보안 분야에서의 주 관심 주제를 확인할 수 있으며, 이러한 주제를 학습하여 차세대 정보 보안 기술을 선도하기 위한 기반이 다질 수 있다.

참 고 문 헌

[1] Kim, J.H., Oh, K.H., Choi, Y.J., Kim, T.S., Choi, D.H. (2013). Technical Trends of Side Channel Analysis System. Electronics and Telecommunications Trends. ETRI, 2013(3), 47-56

[2] Bhasin, S., Breier, J., Hou, X., Jap, D., Poussier, R., & Sim, S. M. (2019). 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(1), 95-122.

[3] Kannwischer, M. J., Pessl, P., & Primas, R. (2020). Single-Trace Attacks on Keccak. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 243-268.

[4] De Meyer, L. (2019). Recovering the CTR_DRBG state in 256 traces. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 37-65.

[5] Genkin, D., Poussier, R., Sim, R. Q., Yarom, Y., & Zhao, Y. (2019). Cache vs. Key-Dependency: Side Channeling an Implementation of Pilsung. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 231-255.

[6] Valiveti, A., & Vivek, S. (2020). Second-Order Masked Lookup Table Compression Scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 129-153.

[7] Sasdrich, P., Bilgin, B., Hutter, M., & Marson, M. E. (2020). Low-Latency Hardware Masking with Application to AES. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2), 300-326.

[8] Gao, S., Marshall, B., Page, D., & Oswald, E. (2019). Share-slicing: Friend or Foe?. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 152-174.

[9] K, K., Roy, I., Rebeiro, C., Hazra, A., & Bhunia, S. (2020). FEDS: Comprehensive Fault Attack Exploitability Detection for Software Implementations of Block Ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2), 272-299.

[10] Zhang, Z., & Liu, P. (2020). A Hybrid-CPU-FPGA-based Solution to the Recovery of Sha256crypt-hashed Passwords. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 1-23.

[11] Krautter, J., Gnad, D., & Tahoori, M. (2020). CPAmap: On the Complexity of Secure FPGA Virtualization, Multi-Tenancy, and Physical Design. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 121-146.

[12] Zaid, G., Bossuet, L., Habrard, A., & Venelli, A. (2019). Methodology for Efficient CNN Architectures in Profiling Attacks. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 1-36.

[13] Hoang, A.-T., Hanley, N., & O'Neill, M. (2020).

Plaintext: A Missing Feature for Enhancing the Power of Deep Learning in Side-Channel Analysis? Breaking multiple layers of side-channel countermeasures. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 49-85.

[14] Zhang, J., Zheng, M., Nan, J., Hu, H., & Yu, N. (2020). A Novel Evaluation Metric for Deep Learning-Based Side Channel Analysis and Its Extended Application to Imbalanced Data. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 73-96.

[15] Bermudo Mera, J. M., Karmakar, A., & Verbauwhede, I. (2020). Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2), 222-244.

[16] Alkim, E., Alper Bilgin, Y., Cenk, M., & Gérard, F. (2020). Cortex-M4 optimizations for {R,M} LWE schemes. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 336-357.

[17] Zhang, N., Yang, B., Chen, C., Yin, S., Wei, S., & Liu, L. (2020). Highly Efficient Architecture of NewHope-NIST on FPGA using Low-Complexity NTT/INTT. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2), 49-72.

[18] Fritzmann, T., Sigl, G., & Sepúlveda, J. (2020). RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 239-280.

[19] Hamburg, M. (2020). Faster Montgomery and double-add ladders for short Weierstrass curves. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 189-208.

[20] Jancar, J., Sedlacek, V., Svenda, P., & Sys, M. (2020). Minerva: The curse of ECDSA nonces : Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 281-308.

[21] Alpirez Bock, E., Amadori, A., Brzuska, C., & Michiels, W. (2020). On the Security Goals of White-Box Cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2), 327-357.

[22] Goubin, L., Rivain, M., & Wang, J. (2020). Defeating State-of-the-Art White-Box Countermeasures with Advanced Gray-Box Attacks. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 454-482.

〈저자소개〉

안 상 우 (SangWoo An)
정회원
2020년 : 국민대학교 정보보안암호수학과 졸업
2020년~현재 : 국민대학교 일반대학원 정보융합보안전공 석사
<관심분야> 정보보호, 융합보안, 암호구현, GPU 보안

송 진 교 (JinGyo Song)
정회원
2020년 : 국민대학교 정보보안암호수학과 졸업
2020년~현재 : 국민대학교 일반대학원 정보융합보안전공 석사
<관심분야> 정보보호, 암호구현, 부채널 분석, 임베디드 보안

박 보 선 (BoSun Park)

정회원

2019년~현재 : 국민대학교 정보보안암호수학과 학부연구생

<관심분야> 정보보호, 암호구현, 웹 보안, 애플리케이션 보안

서 석 충 (Seog Chung Seo)

정회원

2011년 : 고려대학교 공학박사

2011년~2014년 : 삼성전자 책임연구원

2014년~2019년 : 국가보안기술연구소 선임연구원

2019년~현재 : 국민대학교 조교수

<관심분야> 정보보호, 암호구현, 암호모듈검증, 네트워크 보안