TEE 환경에서의 Ciphertext Side-Channel 방어 기법 동향 연구

강기봉 [1], 황윤성 [2], 유준승 [2], 백윤흥 [3]
[1]서울대학교 전기 · 정보공학부 석사과정, 반도체공동연구소
[2]서울대학교 전기 · 정보공학부 석박통합과정, 반도체공동연구소
[3]서울대학교 전기 · 정보공학부 교수, 반도체공동연구소
kbkang@sor.snu.ac.kr, yshwang@sor.snu.ac.kr, jsyou@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study of Defense Against Ciphertext Side-Channel Attacks in Trusted Execution Environments

Ki-Bong Kang[1], Yun-Seong Hwang[1], Jun-Seung You[1], Yun-Heung Paek[1]
[1]Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center (ISRC), Seoul National University

요 약

신뢰 실행 환경(Trusted Execution Environments, TEE) 기술은 Intel SGX, AMD SEV, ARM CCA 등을 중심으로 발전하여, 특권 권한을 가진 공격자로부터 민감한 데이터와 코드를 보호하기 위해 널리 사용되고 있다. 그러나 최근 연구들은 TEE 에서 사용되는 결정론적 메모리 암호화 방식이 Ciphertext Side-Channel Attack 이라는 새로운 유형의 취약점을 초래할 수 있음을 보여주었다. 이러한 공격은 암호화된 메모리의 변화를 관찰함으로써 메모리 보호를 직접적으로 침해하지 않고도 민감한 정보를 추론할 수 있다.

본 연구는 Ciphertext Side-Channel Attack 의 근본적인 원리를 체계적으로 분석하고, TEE 환경에서 이를 완화하기 위해 제안된 최신 방어 기법 동향을 조사하였다. 특히, Enclave Management Task 의 물리적 분리, 성능과 보안성을 균형 있게 확보하는 Hybrid Memory Encryption 기법, 그리고 암호문 패턴 예측을 방지하기 위한 Interleaving 기반 데이터 다양화 전략을 중심으로 하드웨어 기반 주요 대응 방식을 심층적으로 분석하였다.

방어 전략별 강점과 한계를 비교 분석한 결과, 현재의 대응 기법들은 각각 특정 조건에서 효과적이나 모든 공격 시나리오를 포괄하기에는 한계가 있음을 확인하였다. 이에 따라, 지속 가능한 TEE 보안을 위해서는 하드웨어와 소프트웨어의 긴밀한 협력을 기반으로 한 Cross-Layer Co-Design 접근, 세분화된 메모리 은닉화 기법과 비결정론적 암호화 모델이 필수적임을 제안한다.

1. 서론

최근 클라우드 컴퓨팅 및 엣지 컴퓨팅 환경의 확산과 함께, 신뢰할 수 없는 인프라 위에서도 민감한 데이터와 코드를 안전하게 처리할 수 있는 Confidential Computing 에 대한 관심이 급격히 증가하였다. 이를 지원하기 위한 핵심 기술로 Trusted Execution Environment(TEE)가 주목받고 있으며, Intel SGX, AMD SEV, ARM CCA 등 다양한 형태의 TEE 는 하드웨어 기반의 격리 환경을 제공하여 운영체제, 하이퍼바이저, 심지어 시스템 관리자와 같은 권한을 가진 공격자로부터 프로그램과 데이터를 보호할 수 있도록 설계되었다.

TEE 는 공격자로부터 메모리를 보호하기 위해 메모리 암호화를 사용한다. 특히, AMD SEV 계열은 AES-XTS 또는 AES-XEX 모드에 기반하여 메모리를 블록 단위로 암호화하므로써 데이터에 대한 무단 접근을 방지한다. 그러나 Cipherleak [1]에서는 이러한 암호화 방식이 가지는 결정론적 암호문 생성 방식이 심각한 취약점을 초래할 수 있음을 보였다.

Cipherleak 은 암호화된 메모리 내용만 관찰할 수 있는 공격자가 메모리 암호문의 변화 양상을 분석함으로써 평문 데이터의 변화 여부와 기밀 데이터를 유추한다. 이러한 공격은 기존의 캐시 타이밍 공격이나 브랜치 기반 부채널 공격과는 본질적으로 다른 성질을 가지며, 메모리 암호화가 전제하는 데이터 은닉성

가정을 근본적으로 붕괴시킨다.

이에 따라 최근 수년간, 소프트웨어 수준의 완화 기법, 프로그램 흐름 은닉 기법, 하드웨어 아키텍처 수정 등 다양한 대응책이 제안되었다. 그러나 각 방법은 특정 환경에 제한적이거나, 성능 오버헤드와 실용성 사이에서 근본적 tradeoff 를 보인다.

본 논문에서는 이러한 Cipherleak 에서 제시된 취약점을 중심으로,

1. 공격의 근본 원리와 심각성을 명확히 규명하고,
2. 소프트웨어 및 하드웨어 기반 방어 기법을 체계적으로 정리 · 분석하며,
3. TEE 아키텍처 변경을 포함한 하드웨어 수준 대응의 최신 동향을 심층적으로 고찰하고자 한다.

이를 통해 향후 Confidential Computing 시스템이 직면하게 될 보안 요구사항과 설계 방향성을 제시하고자 한다.

2. 관련 연구

2.1 소프트웨어 기반 완화 기법

초기 대응 연구들은 소프트웨어적으로 Cipherleak 을 완화하려는 시도를 진행했다.

Cipherfix [2]는 동적 테인트 추적(Dynamic Taint Tracking)과 바이너리 재작성(binary rewriting)을 결합하여 기밀 데이터가 메모리에 쓰일 때마다 랜덤 마스킹(Masking)을 적용하는 접근을 제안했다. 이를 통해 암호문 중복 문제를 원천적으로 제거하려 하였으나, 랜덤 마스크 생성 및 저장 연산 추가로 인해 최대 16.8 배의 성능저하가 발생하는 단점이 있다.

CipherGuard [3]는 컴파일러 단계에서 미리 기밀 데이터의 메모리 저장을 탐지하고, 최적화된 난수 기반 변형을 적용하는 LLVM 기반의 프레임워크를 제시하여, 분석 범위가 넓고 성능에 대한 최적화를 통해 평균 1.7~3.1 배 가량의 오버헤드만으로 완화 기법 적용에 성공하였다. 하지만 복잡한 컴파일 환경과 소스코드가 반드시 필요하다는 단점이 있다.

Obelix [4]는 중요한 코드 및 데이터를 ORAM(Oblivious RAM) 기법으로 블록화 및 난독화 하여, 코드 및 데이터 흐름을 은닉하는 방식을 제안했다. 이 방식을 통해 Single-Stepping 과 Ciphertext Side-Channel Attack 에 대한 방어가 가능했으나, ORAM 적용에 의한 메모리 접근 증가로 성능저하가 극심하다는 단점이 있다.

2.2 하드웨어 기반 완화 기법

소프트웨어 기반 완화 기법의 한계가 확인되면서, 하드웨어 수준의 아키텍처 개선을 통한 대응 연구가 등장하였다.

HyperTEE [5]는 기존 TEE 의 문제점을 지적하며 Enclave management task 를 별도의 Enclave Management Subsystem(EMS)으로 완전히 분리하는 아키텍처를 제안했다. Management task 가 연산 영역에서 분리됨에 따라 attack surface 가 감소하고, 인증, 메모리 관리, 통신 등을 안전하게 수행할 수 있게 변경되었다. FPGA 프로토타입에서 동작 및 성능을 검증하였고, Enclave workload 대비 2% 이내의 오버헤드를 확인하였다.

Counter-light Memory Encryption [6]은 Counter Mode 와 Counterless Mode 를 결합하여 메모리 암호화의 성능 저하 문제를 해결하는 방안을 제안했다. 필요에 따라 counter 적용 여부를 판단하고 상황에 맞는 방식을 적용하여 성능을 최적화하였다. 메모리 대역폭이 최적화되고, 성능을 98% 가량 유지하였으나, 일부 corner case 에 여전히 취약하다는 단점이 있다.

ZEBRAFIX [7]는 데이터 블록 내부에 counter 와 실제 데이터를 섞어 저장하는 방식(interleaving)을 제안하여, 암호문 패턴 중복을 방지하는 구조적 변형을 시도했다. 8-byte 단위로 counter 를 삽입하여 암호문 다양성(ciphertext diversity)을 강화하였다. 기존의 마스킹(Masking) 기법 대비 낮은 오버헤드를 보이지만, non-linear access 패턴 등의 문제에 취약하다는 단점이 있다.

3. 기존 완화 기법 분석

TEE 환경에서의 Ciphertext Side-Channel 공격에 대응하기 위한 완화 기법은 크게 소프트웨어 기반과 하드웨어 기반으로 구분된다. 본 장에서는 기존에 제안된 대표적인 대응 기법들을 범주별로 정리하고, 각 기법의 장단점을 비교한 뒤 향후 보완이 필요한 연구 방향을 제안한다.

3.1 소프트웨어 기반 완화 기법의 특징과 한계

소프트웨어 기반 대응은 시스템의 범용성과 이식성이 뛰어나며, 하드웨어 변경 없이도 적용 가능하다는 장점을 가진다. 그러나 마스킹 연산 또는 난독화 기법은 높은 성능 오버헤드를 유발하며, 소스코드 접근이 어려운 경우 적용이 제한된다. 또한, 보안 수준 면에서도 하드웨어 기반 접근에 비해 상대적으로 낮을 수 있다.

3.2 하드웨어 기반 완화 기법의 특징과 한계

하드웨어 기반 대응 기법은 높은 보안성과 낮은 탐지 가능성을 제공하여 보다 근본적인 차단 효과를 기대할 수 있다, 그러나 새로운 하드웨어 자원을 필요로 하며, 기존 아키텍처와의 호환성 문제, 설계 복잡도, 적용 비용 등의 현실적 제약이 뒤따른다. 특히, 물리적 자원 분리나 암호화 구조 변경과 같은 접근은 corner case 에 대한 세심한 고려가 필요하다.

3.3 기존 기법의 비교 및 향후 연구 방향

표 1 은 기존의 주요 완화 기법들을 분류별로 정리한 것으로, 각 접근 방식이 갖는 특성과 한계를 한눈에 파악할 수 있다. 이를 통해 확인할 수 있듯, 현재의 대응 기법들은 특정 조건에서는 효과적일 수 있으나, 모든 공격 시나리오에 일관되게 적용하기에는 한계가 존재한다.

이에 따라 향후 연구는 다음과 같은 방향에 집중할

연구명	방어 기법	주요 특징	장점	한계
Cipherfix[2]	동적 마스킹 및 바이너리 변조	기존 바이너리에 적용 가능, 실행 중 탐지	높은 범용성	극심한 성능 저하
CipherGuard[3]	컴파일러 기반 마스킹 삽입	컴파일 타임 탐지 및 최적화 가능	성능 최적화 가능	소스코드 접근 필요, 재컴파일 필요
Obelix[4]	ORAM 기반 난독화	코드 및 데이터 흐름 모두 은닉	높은 보안성	메모리/성능 오버헤드
HyperTEE[5]	EMS 를 통한 관리 채널 보안성 확보	Enclave 관리 채널을 하드웨어에서 분리	관리 프로세스 보호	하드웨어 비용 상승
Counter-light[6]	Hybrid Memory Encryption	Counter 사용을 최소화하여 성능 유지	높은 성능	일부 공격 모델에 대한 취약점 존재
ZEBRAFIX[7]	데이터-카운터 Interleaving	저장 구조 변형을 통한 암호문 다양화	낮은 오버헤드	일부 데이터 패턴에 취약

표 1. 주요 연구 간 방어 기법 비교

필요가 있다.

- **Cross-layer Co-Design:** 하드웨어와 소프트웨어가 협력하는 통합 방어 구조를 설계하여 상호 보완성을 높이고, 성능과 보안을 균형 있게 유지할 수 있어야 한다.
- **비결정론적 암호화 및 은닉화 기법:** 결정론적 암호화 방식이 가지는 근본적 한계를 극복하기 위해, 데이터 접근 패턴을 은닉하고 암호문 다양성을 보장하는 새로운 메커니즘이 필요하다.

결국, 단일 계층에 의존하지 않는 복합적이고 유연한 방어 전략이 지속 가능한 TEE 보안을 위한 핵심 요소가 될 것이다.

4. 결론 및 향후 과제

Confidential Computing 의 상용화가 본격화되면서, 기존 TEE 시스템은 Ciphertext Side-Channel 공격이라는 새로운 유형의 위협에 직면하고 있다. 본 논문에서는 이러한 공격의 원리를 분석하고, 이를 완화하기 위한 기존의 소프트웨어 및 하드웨어 기반 대응 기법들을 체계적으로 고찰하였다.

현존하는 대응 전략은 각기 다른 접근 방식에 따른 한계를 갖는다. 소프트웨어 기반의 마스킹 및 난독화 기법은 높은 성능 오버헤드를 초래하거나 적용 가능성에 제약이 있으며, 하드웨어 아키텍처를 수정하는 방식은 강력한 방어 효과를 제공하는 반면, 설계 복잡성과 적용 비용 증가라는 현실적인 부담이 따른다.

이에 따라 향후 연구는 메모리 접근 패턴을 구조적으로 은닉할 수 있는 정교한 방어 메커니즘의 개발과 함께, 암호문 반복성과 패턴 노출을 원천적으로 차단할 수 있는 비결정론적 암호화 기반 최적화 기법의 설계가 필요하다. 아울러, 운영체제와 하드웨어가 긴밀히 협력하는 cross-layer 방어 프레임워크를 통해, 보안성과 성능 간 균형을 갖춘 지속 가능한 대응 방안을 마련해야 한다. 이러한 다층적이고 유연한 접근은 향후 TEE 시스템의 신뢰성과 실용성을 확보하는 핵심이 될 것이다.

ACKNOWLEDGEMENT

이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (RS-2023-00277326). 이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2023-RS-2023-00256081). 이 논문은 2025 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음. 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다. 이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00528, 하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발)

참고문헌

[1] Li, Mengyuan, et al. "{CIPHERLEAKS}: Breaking constant-time cryptography on {AMD}{SEV} via the ciphertext side channel." 30th USENIX Security Symposium (USENIX Security 21). 2021.

[2] Wichelmann, Jan, et al. "Cipherfix: Mitigating ciphertext {Side-Channel} attacks in software." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

[3] Jiang, Ke, et al. "CipherGuard: Compiler-aided Mitigation against Ciphertext Side-channel Attacks." arXiv preprint arXiv:2502.13401 (2025).

[4] Wichelmann, Jan, et al. "Obelix: Mitigating side-channels through dynamic obfuscation." 2024 IEEE Symposium on Security and Privacy (SP). IEEE, 2024.

[5] Bai, Yunkai, et al. "HyperTEE: A Decoupled TEE Architecture with Secure Enclave Management." 2024 57th IEEE/ACM International Symposium on Microarchitecture (MICRO). IEEE, 2024.

[6] Wang, Xin, et al. "Counter-light Memory Encryption." 2024 ACM/IEEE 51st Annual International Symposium on Computer Architecture (ISCA). IEEE, 2024.

[7] Pätschke, Anna, Jan Wichelmann, and Thomas Eisenbarth. "Zebrafix: Mitigating Memory-Centric Side-Channel Leakage via Interleaving." arXiv preprint arXiv:2502.09139 (2025).